◄ آخرین یافته‌های اچ‌بی‌آر
درباره آینده کسب‌وکارها

Insights You Need from
Harvard Business Review

امنیت سایبری

بهسازان ملت
behsazan mellat
انتشارات راه‌پرداخت

انتشارات راه پرداخت


بسم الله
الرحمن
الرحيم

١ ٣ ٩ ٩

Harvard Business Review

امنیت سایبری

بینش‌هایی از مجله کسب‌وکار هاروارد

بهسازان ملت
behsazan mellat

انتشارات راه‌پرداخت

عنوان قراردادی: هاروارد بیزنیس ریویو (مجله) Harvard Business Review/عنوان و نام پدیدآور: امنیت سایبری: بینش هایی از مجله کسب و کار هاروارد/گروه نویسندگان مجله کسب و کار هاروارد/مترجم فاطمه کشت ورز/مشخصات نشر: تهران: راه پرداخت، ۱۳۹۹./مشخصات ظاهری: ۱۲۰ ص.؛ ۱۴/۵×۲۱/۵ س م./شابک: ۵-۱-۹۷۲۲۰-۶۲۲-۹۷۸/وضعیت فهرست نویسی: فیپا/ یادداشت: عنوان اصلی:./. [2019], Cybersecurity: the insights you need from Harvard Business Review: عنوان دیگر: بینش هایی از مجله کسب و کار هاروارد./ موضوع: کامپیوترها - ایمنی اطلاعات/موضوع: Computer security/موضوع : شرکت های اقتصادی - تدابیر ایمنی/موضوع: Business enterprises - Security measures/شناسه افزوده: کشت ورز، فاطمه، ۱۳۷۸ -، مترجم/شناسه افزوده: سرافرازی، قاسم، ۱۳۶۶ -، ویراستار/رده بندی کنگره: QA۷۶/۹/رده بندی دیویی: ۰۰۵/۸/ شماره کتابشناسی ملی: ۷۲۷۱۵۳۵

Cybersecurity: The Insights You Need from Harvard Business Review (HBR Insights Series)
by Harvard Business Review (Author), Alex Blau (Author), Andrew Burt (Author), Boris Groysberg (Author), Roman V. Yampolskiy (Author)
2019

چرا از کاغذ بالکی استفاده می کنیم ؟

۱. کاغذ بالکی از کاغذهای تحریر سفید، سبک تر است
۲. در تهیه آن از مواد شیمیایی استفاده نشده و شیوه تولید آن مکانیکال است
۳. نور را منعکس نمی کند و مانع از خستگی چشم هنگام مطالعه می شود

* کاغذ بالکی به دلیل موارد بالا از کاغذ تحریر سفید گران تر است

امنیت سایبری

بینش‌هایی از مجله کسب‌وکار هاروارد

نویسندگان:
الکس بلو
اندی بوچمن
اسکات برینا‌تو
مت پری

مترجم:
فاطمه کشت‌ورز

بهسازان ملت
behsazan mellat

انتشارات راه‌پرداخت

امنیت سایبری/ناشر: راه‌پرداخت/نویسنده: گروه نویسندگان مجله کسب‌کار هاروارد/ویراستار محتوایی: قاسم سرافرازی/ویراستار: یلدا شایسته‌فر/صفحه‌آرا: علیرضا کیوان/نوبت چاپ: اول ۱۳۹۹/شمارگان: ۱۰۰۰ نسخه شابک: ۵-۱-۹۷۲۲۰-۶۲۲-۹۷۸/

وب‌سایت: shop.way2pay.ir

فهرست

[یادداشت حامی]

امنیت سایبری از مفاهیمی است که به اندازه کافی مورد توجه قرار نگرفته است. امنیت یک زیرساخت است؛ مثل اینترنت، شبکه، حمل‌ونقل، برق، آب، گاز و هر بستر دیگری که بشر آن را برای زیست بهتر خود توسعه داده است. در جهانی که امنیت وجود نداشته باشد، هیچ فعالیت سالم و سازنده‌ای قابل انجام و پیگیری نیست. اکنون که شبکه‌های کامپیوتری گسترش یافته‌اند و جهان دیجیتال به بخشی از زندگی روزمره تبدیل شده، همه ما در جهان سایبر ـ فیزیکی زندگی می‌کنیم. همان‌گونه که امنیت در جهان فیزیکی اهمیت دارد، در جهان سایبری هم مقوله مهمی است که متأسفانه به اندازه کافی جدی گرفته نشده است.

امنیت سایبری (امنیت رایانه‌ای یا امنیت فناوری اطلاعات) یعنی حفاظت از سامانه‌های اطلاعاتی در برابر آسیب به سخت‌افزار، نرم‌افزار و اطلاعات نرم‌افزاری؛ امنیت سایبری مقوله‌هایی مانند محافظت در برابر حمله محروم‌سازی از سرویس (اختلال) و بات‌نت‌ها (گمراهی) را هم در بر می‌گیرد.

متأسفانه در موضوع امنیت سایبری آنچه کمتر به آن توجه می‌شود، رخنه‌پذیری از طریق منابع انسانی است. ممکن است کسب‌وکارها موضوع امنیت را صرفاً موضوعی فنی ببینند و تصور کنند که با خرید تجهیزات پیشرفته می‌توانند امنیت را برقرار کنند، در حالی که بیشتر رخنه‌های امنیتی از طریق منابع انسانی سازمان‌ها صورت می‌گیرد.

با توجه به افزایش وابستگی به سامانه‌های رایانه‌ای و اینترنت در بیشتر جوامع، شبکه‌های

بی‌سیم مانند بلوتوث و وای‌فای و رشد دستگاه‌های هوشمند مانند تلفن هوشمند، تلویزیون و دستگاه‌های کوچک مانند اینترنت اشیا؛ امنیت سایبری اهمیت روبه‌رشدی پیدا کرده است.

تهدیداتی مانند جرائم مجازی، آسیب‌پذیری، شنود، بدافزار، جاسوس‌افزار، باج‌افزار، تروجان، ویروس‌ها، کرم‌رایانه‌ای، روت‌کیت‌ها، کی‌لاگرها، تراش‌دادن داده، اکسپلویت، درب پشتی، بمب منطقی و حمله محروم‌سازی از سرویس، هر روز نقش جدی‌تری در زندگی سایبر ـ فیزیکی پیدا می‌کنند. کوچک‌ترین اختلالی در فعالیت‌های سایبری به آسیب‌های جدی در دنیای فیزیکی منجر می‌شود. نمی‌توان انتظار داشت که بدون در نظر گرفتن روال‌های امنیتی شاهد این باشیم که امنیت سایبری برقرار شود. با در نظر گرفتن این موضوع مهم که امنیت یک مفهوم نسبی است، پیچیدگی این حوزه بیشتر هم می‌شود.

نویسندگان کتاب امنیت سایبری معتقدند که شرکت‌ها دو دسته هستند؛ آنهایی که هک شده‌اند و آنهایی که در آینده هک می‌شوند! با این نگاه طبیعی است که مدیران سازمان‌های امروز باید خودشان را برای پس از هک آماده کنند! نه تنها برای هک نشدن؛ بلکه برای بعد از هک نیز باید آماده باشیم. همه کسب‌وکارهای بزرگ و کوچک امروز جهان در معرض هک‌شدن قرار دارند. انواع آسیب‌پذیری‌ها، سیستم‌های سایبری را تهدید می‌کند و تلاش برای کتمان رخنه‌ها صرفاً به عمیق‌تر شدن شکاف‌ها منجر می‌شود. سیستم‌های نرم‌افزاری و سخت‌افزاری امروز به‌صورت پیوسته باید ارتقا یابند تا هکرها یک قدم عقب‌تر باشند، ولی نکته مهم‌تر و بعضاً فراموش‌شده این است که نه تنها سیستم‌های سخت‌افزاری و نرم‌افزاری؛ بلکه منابع انسانی نیز به‌صورت پیوسته

باید تحت آموزش قرار بگیرند. روش‌های قدیمی، دیگر پاسخگو نیست و ما نمی‌توانیم انتظار داشته باشیم که با روش‌های تاریخ‌مصرف‌گذشته امنیت سایبری را تأمین کنیم.

آموزه‌های این کتاب بسیار ساده و به‌غایت کاربردی است. دیدگان شما را دعوت می‌کنیم به صفحات آتی این کتاب، به این امید که بهره لازم برای غنی‌تر کردن رویکردهای ارتقای امنیت در سازمان شما نیز حاصل آید.

شرکت بهسازان ملت

[یادداشت ناشر]

امروزه موضوع امنیت سایبری به یک مسئله حیاتی برای کسب‌وکارها تبدیل شده، اما هنوز هم هستند کسب‌وکارهایی که تا وقتی با مشکل امنیتی و نشت داده‌های خود مواجه نشده‌اند، اهمیت امنیت سایبری را درک نمی‌کنند. طبق یک نقل قول معروف از کارشناسان امنیتی، نشت داده بالأخره اتفاق می‌افتد و هکرها راهی خواهند یافت تا به سیستم‌های یک شرکت نفوذ کنند. اما نکته بااهمیت میزان خسارتی است که پس از این اتفاق به بار می‌آید. به عبارت دیگر حمله سایبری و نشت داده در دنیای کنونی گریزناپذیر است و فقط با آمادگی قبلی و اتخاذ رویکردهای صحیح امنیتی می‌توان از میزان خسارت آن کاست. البته همچنان یک راه وجود دارد که بتوانیم تا حد زیادی خودمان را از شر حملات سایبری رها کنیم؛ اینکه از کامپیوترها استفاده نکنیم. همان‌طور که در یکی از مقالات کتاب و به نقل از «ویلیس ویر» از پیشگامان حوزه امنیت و حریم خصوصی چنین جمله‌ای آمده است: «تنها کامپیوتری که به‌طور کامل امن است، کامپیوتری است که کسی از آن استفاده نمی‌کند.»

بزرگ‌ترین شرکت‌های فناوری با این مسئله در سطح وسیع مواجه شده‌اند. شرکت یاهو در سال ۲۰۱۶ هدف حمله وسیع سایبری قرار گرفت و اطلاعات سه میلیارد کاربرش به دست هکرها افتاد. شرکت مایکروسافت نیز انگشت اتهام را به سمت هکرهای چینی در خصوص هک‌شدن ایمیل‌های این شرکت نشانه رفته است. همین چند ماه پیش بود که هک حساب افراد مشهور در توییتر و درخواست بیت‌کوین از کاربران سروصدای زیادی به پا کرد. نمونه‌های داخلی فراوانی

را هم می‌توان به‌عنوان نمونه ذکر کرد. از هک اطلاعات شـــرکت رایتل گرفته تا هک وب‌سایت سازمان تأمین اجتماعی و هک سیستم‌های بندر شهید رجایی از جمله مواردی است که صرفاً در سال جاری صورت پذیرفته است. همه این موارد اهمیت بهداشت سایبری را برجسته می‌کنند.

اینکه چه اقداماتی انجام دهید که قربانی یک حمله سایبری بزرگ در شرکت و سازمان خود نشوید یا اگر در معرض چنین واقعه‌ای قرار گرفتید، چه اقداماتی انجام دهید، از جمله مهم‌ترین مسائلی اســـت که باید هر مدیر یا رهبر کسب‌وکاری برای آن آماده باشـــد و تمهیداتی برای آن بیندیشد.

این کتاب به ما از اشتباهات تکراری مدیران پس از وقوع یک حمله سایبری می‌گوید. از اینکه منابع انسانی سازمان و آموزش آنان مهم‌ترین سد جهت جلوگیری از وقوع یک حمله سایبری هستند. کتاب از این صحبت می‌کند که مدیران چطور در حرف از اهمیت سایبری می‌گویند، اما در عمل آن را جدی نمی‌گیرند یا اینکه اصلاح عادات غلط کارکنان در حوزه امنیتی می‌تواند مانع یک فاجعه شود.

کتاب امنیت سایبری بر خلاف تصور کتابی خواندنی و جذاب است که نه‌تنها به ما هشدار می‌دهد که امنیت ســـایبری را جدی بگیریم؛ بلکه راهکار ارائه می‌دهد. امیدواریم انتشار این کتاب بتواند گامی هرچند کوچک در راســـتای بالا بردن حساسیت‌ها نسبت به موضوع امنیت سایبری در کشورمان باشد.

قاسم سرافرازی
انتشارات راه‌پرداخت

مقدمه

اکنون همه مادر گیر این مساله هستیم

الکس بلو[1]

زمانی اینترنت تنها یک ایده محض بود؛ آینده‌ای به‌ظاهر غیر قابل تصور که در آن همه‌چیز و همه‌کس با هم ارتباط پیدا می‌کردند. تصور بر این بود که در چنین دنیایی جریان‌های بدون وقفه از اطلاعات و داده‌ها، پیشرفتی بی‌سابقه را در ارتباطات، سلامت، حمل‌ونقل، اتوماسیون و تجارت رقم بزنند و البته در این دنیا نقشی برای ربات‌ها هم در نظر گرفته می‌شد. دنیای امروز ما چندان دور از این تصورها نبوده و همین فناوری‌ها هستند که نحوه عملکرد شرکت‌ها و دولت‌ها را از اساس تغییر داده‌اند. در میان این رویاهای شیرین، متخصصان امنیت هشدار داده‌اند که این دنیای به‌هم‌پیوسته ما می‌تواند خطرآفرین هم باشد. هکرها، هوش مصنوعی پیشرفته و بازیگران بد در دولت‌ها و ابرشرکت‌ها تهدیدهای قابل توجهی برای زندگی روزمره ما هستند. حتی بهترین آرمانشهر سایبری هم می‌تواند یک دنیای شیطانی زیرزمینی در درون خود داشته باشد.

امروزه در دنیای واقعی، همان فناوری‌های مفید، پیامدهای جدید و متغیری را برای امنیت سایبری افراد، شرکت‌ها و دولت‌ها به وجود آورده‌اند. این پیامدها می‌توانند به‌سادگی ایجاد رمز عبوری جدید و سخت پس از نفوذ اطلاعاتی باشند یا می‌توانند ریسک‌هایی ترسناک باشند؛ مانند اینکه دشمنی خارجی بتواند چراغ‌های خیابان را خاموش کند یا سیستم‌های تصفیه آب را از کار بیندازد یا حتی به زیرساخت‌های نظامی غلبه کند.

هرچند مدیریت این ریسک‌ها از قدیم به عهده کارشناسان و تکنیسین‌ها بوده است، اما دیگر نمی‌توان حوزه امنیت سایبری را به متخصصان فناوری اطلاعات محدود کرد. در عوض همه ما مدیران، چه در سازمان‌های خصوصی و چه در سازمان‌های دولتی، باید به نقش امنیت سایبری در وظایف و مسئولیت‌هایمان پی ببریم و خود را در زمینه تغییرات ریسک‌ها در امنیت سایبری به‌روز نگه داریم. این کتاب به افراد غیرحرفه‌ای کمک می‌کند تا به‌سرعت، درکی عمیق از حوزه امنیت سایبری به دست آورند. این کتاب چند موضوع بسیار مهم را پوشش می‌دهد و مطالعه

1. Alex Blau

آن دو مزیت برای شما دارد؛ اول اینکه با مسائل فعلی و مسائل آتی در حوزه امنیت سایبری آشنا می‌شوید؛ مسائلی که با نقش، سازمان و صنعت شما مطابقت دارند. دوم اینکه متوجه خواهید شد که هم بخشی از مشکلات امنیتی سازمان هستید و هم نقشی کلیدی در شناسایی و مدیریت راه‌حل‌های امنیتی ایفا می‌کنید.

تعداد صنایعی که برای تعیین استراتژی و مدیریت عملیات خود به جمع‌آوری داده و اطلاعات در مورد تمام جوانب کسب‌وکار، به‌ویژه مشتری‌ها وابسته‌اند، هر روز بیشتر می‌شود. هرچند دسترسی به چندین پتابایت داده، بهره‌وری عملیاتی را بهبود می‌بخشد و فرصت‌های جدیدی به وجود می‌آورد، اما این حجم عظیم داده می‌تواند خسارت‌هایی نیز برای شرکت‌ها و افراد به همراه داشته باشد. اکنون حمله‌های سایبری و نفوذ اطلاعاتی رواج یافته و هر ساله پرحجم‌تر و پرهزینه‌تر می‌شوند و با وجود توانایی روزافزون ما در جلوگیری از این حمله‌ها و بالا بردن فناوری امنیت و بهداشت سایبری، این نفوذها کاهش نیافته است. باید انتظارات خود را از توانایی‌هایمان بالا ببریم، این ریسک‌ها را کاهش دهیم و بپذیریم که نفوذهای اطلاعاتی اجتناب‌ناپذیر هستند.

از زمانی که اطلاعات مشتری برای هکرها ارزشمندتر شده و دولت‌ها قوانینی را برای جریمه شرکت‌ها، به علت از دست دادن اطلاعات مشتری یا نفوذ به آن، وضع کرده‌اند، شرکت‌هایی که حضور اینترنتی دارند و اطلاعات مشتریان را جمع‌آوری می‌کنند با ریسک‌های بیشتری مواجه شده‌اند؛ اما این نکته دیگر فقط در مورد بانک‌ها و سازمان‌های خدمات مالی صدق نمی‌کند.

این پارادایم جدید نیازمند یک طرز فکر متفاوت است و این کتاب به رهبران غیرفنی، از جمله مدیران اجرایی، اعضای هیات‌مدیره و سایر مسئولان در تنظیم قوانین؛ از طراحی و بازاریابی گرفته تا منابع انسانی و حسابداری، با هدف سرعت‌بخشیدن به وضعیت فعلی این حوزه کمک می‌کند. کتاب امنیت سایبری اصول مقدماتی را معرفی می‌کند و در عین حال به موضوعاتی چون نحوه مشارکت هیات‌مدیره و مدیران اجرایی در حوزه امنیت سایبری، سرمایه‌گذاری و تصمیم‌گیری در این حوزه، اهمیت تعیین عوامل انسانی در امنیت سایبری و اینکه چرا همه اعضا باید در این رابطه نقشی ایفا کنند، ارتباطات و عکس‌العمل مناسب در پی نقض داده‌ها، دفاع فعال و اصول «هک متقابل»[1]، ارزش رو به فزونی حریم خصوصی در امنیت سایبری، ملاحظات امنیت سایبری برای تجارت بین‌الملل و نیز آینده هوش مصنوعی در امنیت سایبری نگاه ویژه‌ای دارد. این موارد

1. Hacking back

منتخب به درک‌تان در انتخاب مشاور مناسب در مورد مسائل حیاتی، هم‌سطح ماندن با رقبا و همکاران و شناسایی اثرات بالقوه بر تیم، سازمان و صنعتی که در آن فعال هستید، کمک می‌کند. همچنین خواندن این کتاب به شـــما کمک خواهد کرد تا تشخیص دهید سازمان شما در آینده چگونه باید برای همراه‌شدن با جریان‌های امنیت سایبری پیشرفت کند.

این کتاب صرفا بیانگر آغاز راه است. امنیت سایبری هنوز یک حوزه نسبتا جدید است که خود را به‌صورت پویا با تغییرات محیط رگولاتوری نوپا و توسعه فناوری‌های جدید تطبیق خواهد داد. برخی از این تغییرات به‌سود تمامی افراد جامعه خواهد بود. به‌عنوان مثال، در حال حاضر مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR) شـــرکت‌ها را بـــه رعایت اقدامات احتیاطی بیشتر و مراقبت از داده‌های مشتری ترغیب و از مدل‌های کسب‌وکاری که متکی بر فروش چنین داده‌هایی به اشخاص ثالث هستند جلوگیری می‌کند. با این حال، دیگر تغییرات، مانند پیشرفت‌ها در حوزه هوش مصنوعی و محاسبات کوانتومی، تهدیدهای جدید و بالقوه‌ای را به وجود خواهند آورد که می‌توانند اقدامات فعلی ما در حوزه امنیت سایبری را کم‌ارزش کنند و برای کسب‌وکارها و دولت‌ها مشـــکلاتی به وجود بیاورند. درک این ریسک‌ها و فرصت‌های جدید برای موفقیت شرکت‌ها و همچنین به‌طور کلی حفاظت از مردم و جامعه در آینده حیاتی خواهد بود.

حوزه امنیت ســـایبری صرفا متعلق به آینده‌پژوهان فناوری و بومیان دیجیتال نیســـت. همه ما چه بخواهیم و چه نخواهیم به این دنیای جدید وارد شـــده‌ایم. همه ما (جامعه جهانی) باید دست‌به‌دست یکدیگر دهیم تا از رخداد یک فاجعه مرتبط با فناوری جلوگیری کنیم. لازم است این مساله برای همگان روشن شود که تک‌تک افراد جامعه درگیر این مساله هستند و باید برای رفع تهدیدهای این حوزه نقش خود را ایفا کنند.

۱. ناامنی اینترنت

اندی بوچمن

این یک حقیقت تلخ اســت؛ اهمیتی ندارد که ســازمان شــما چه مقدار برای جدیدترین سخت‌افزارها و نرم‌افزارها، آموزش و همچنین منابع انسانی در حوزه امنیت سایبری هزینه کرده یا اینکه سیستم‌های پایه‌ای خود را از ســایر سیستم‌ها جدا کرده باشد. اگر سیستم‌های حیاتی که در راستای ماموریت سازمان‌تان قرار دارند، دیجیتالی و به طریقی به اینترنت متصل باشند (به احتمال زیاد متصل هستند، حتی اگر شــما طور دیگری فکر کنید)، آنها هرگز نمی‌توانند کاملا ایمن شوند.

این مساله حائز اهمیت است، چون در حال حاضر سیستم‌های دیجیتال و متصل به اینترنت به‌صورت مجازی در هر بخشــی از اقتصاد ایــالات متحده نفوذ دارند و در ســال‌های اخیر پیچیدگی فعالیت‌های خرابکارانه و عاملان آنها (اعم از گروه‌های تحت حمایت دولت‌های مرکزی، سازمان‌های جنایی و گروه‌های تروریستی) بسیار زیاد افزایش یافته است.

حملات رخ‌داده در ایالات متحده علیه دولت محلی آتلانتا و علیه یک شبکه داده[1] مشترک بین چهار اپراتور خطــوط لوله گاز، ســرقت داده‌ها از «آکوئیفاکــس» و حملات بدافزاری «واناکرای»[2] و «نات‌پتیا»[3] را ملاحظه کنید. در مورد بسیاری از حوادث شناخته‌شده سال‌های اخیر، شرکت‌های قربانی نشت داده تصور می‌کردند که سیستم دفاع سایبری قدرتمندی دارند.

من عضو یک تیم در آزمایشــگاه ملی آیداهو (INL) هستم که در حال بررسی این موضوع اســت که ســازمان‌های حیاتی برای اقتصاد و امنیت ملی ایالات متحده چگونه می‌توانند به بهترین شکل از خود در برابر حملات ســایبری محافظت کنند. تمرکز ما روی سامانه‌هایی بود که به سیستم‌های کنترل صنعتی (مانند آنهایی که گرما و فشــار را در ابزارهای الکتریکی و پالایشــگاه‌های نفت تنظیم می‌کنند) وابســته‌اند و راهکاری ارائه دادیم کــه با هیچ‌یک از

1. Data network
2. WannaCry
3. NotPetya

راهکارهای سنتی همخوانی نداشت: «کارکردهایی که اگر دچار نقص شوند، کسب‌وکار شما را به خطر می‌اندازند، شناسایی کنید، آنها را تا حد ممکن از اینترنت جدا کنید، وابستگی آنها به فناوری‌های دیجیتال را تا کمترین میزان ممکن کاهش دهید و پایش و کنترل آنها را از طریق دستگاه‌های آنالوگ و افراد مورد اعتماد پشتیبانی کنید.»

اگرچه روش ما هم چنان در مرحله آزمایشی است، اما سازمان‌ها می‌توانند بسیاری از اصول این رویکرد را هم‌اکنون نیز اعمال کنند.

مسلما، این راهبرد (که برای کسب‌وکارهای کاملا مبتنی بر اطلاعات امکان‌پذیر نیست) ممکن است هزینه‌های عملیاتی را افزایش و در بعضی موارد کارایی را کاهش دهد؛ اما تنها راهی است که می‌توانیم اطمینان پیدا کنیم که سیستم‌های حیاتی از طریق ابزارهای دیجیتال مورد حمله قرار نگیرند. در این فصل، من روش‌های این آزمایشگاه برای شناسایی چنین سیستم‌هایی را ارائه خواهم کرد. حملات معمولا از طریق کارکردها یا فرایندهای آسیب‌پذیری رخ می‌دهند که رهبران هرگز فکر نمی‌کردند این‌قدر حیاتی باشند که مختل کردن آنها بتواند به از کار افتادن سازمان‌شان منجر شود. ما در سال‌های اخیر از اصول این روش در شرکت‌ها و ارتش ایالات متحده استفاده کرده‌ایم و یک طرح آزمایشی یک‌ساله بسیار موفقیت‌آمیزی از این رویکرد را در شرکت «Florida Power & Light» که یکی از بزرگ‌ترین شرکت‌های خدمات الکتریکی ایالات متحده است، اجرا کرده‌ایم. هم‌اکنون دومین طرح آزمایشی در یکی از مراکز نظام‌وظیفه ایالات متحده در حال انجام است. همچنین آزمایشگاه ملی آیداهو در جست‌وجوی راهی برای متداول‌کردن این فرایند است. این موضوع احتمالا به معنای مشارکت با شرکت‌های خدمات مهندسی منتخب و اعطای مجوز و آموزش به آنها جهت اعمال این روش خواهد بود.

تهدید موجود

در سال‌های دور، پمپ‌های مکانیکی، کمپرسورها، شیرفلکه‌ها، رله‌ها و عملگرهای مکانیکی در شرکت‌های صنعتی به کار گرفته می‌شدند. آگاهی موقعیتی از گیج‌های آنالوگ[1] و مهندسان ماهر و مورد اعتمادی که از طریق مدار تلفن ثابت با دفتر مرکزی در ارتباط بودند،

1. Analog gauges

حاصل می‌شد. به غیر از دستکاری زنجیره تامین یا همکاری با یکی از کارکنان، تنها راهی که یک خرابکار می‌توانست عملیات یک شرکت را مختل کند، این بود که به کارخانه وارد شود و از سه ستون فیزیکی امنیتی عبور کند؛ گیت‌ها، نگهبانان و سلاح‌ها.

امروزه عملیات در ۱۲ بخش از ۱۶ بخش زیرساختی که وزارت امنیت داخلی ایالات متحده آنها را حیاتی قلمداد کرده است[۱]، به‌صورت نسبی یا کامل به سیستم‌های کنترل و ایمنی دیجیتال وابسته هستند. هرچند فناوری‌های دیجیتال قابلیت و کارایی شگفت‌انگیزی را به ارمغان می‌آورند، اما ثابت شده که بسیار در معرض حملات سایبری قرار دارند. نقاط ضعف سیستم‌های شرکت‌های بزرگ، آژانس‌های دولتی و موسسات دانشگاهی دائما توسط خرابکاران و با استفاده از ابزارهای خودکاری که به‌راحتی در وب تاریک در دسترس هستند، مورد بررسی قرار می‌گیرند؛ بسیاری از این ابزارها رایگان هستند و قیمت نمونه‌های پیشرفته به صدها یا هزاران دلار می‌رسد (گران‌ترین آنها حتی با پشتیبانی فنی همراه است). اغلب آنها می‌توانند توسط تیم‌های امنیت سایبری باتجربه خنثی شوند، اما در حقیقت دفاع در برابر حملات برنامه‌ریزی‌شده و هدفمند که (اگر نگوییم سال‌ها) ماه‌ها طراحی آن طول کشیده، تقریبا غیرممکن است.

اثرات مالی حملات سایبری رو به افزایش است. تنها دو حمله واناکرای و نات‌پتیا در سال ۲۰۱۷، به‌ترتیب خساراتی بالغ بر چهار میلیارد دلار و ۸۰۰ میلیون دلار در بر داشتند. طبق گزارش‌ها در حمله واناکرای که ایالات متحده و بریتانیا، کره شمالی را به دست‌داشتن در آن متهم کردند، از ابزارهای به‌سرقت‌رفته از آژانس امنیت ملی استفاده شده بود. این باج‌افزار برای حمله از یک شکاف در دستگاه‌های مبتنی بر ویندوزی که پچ امنیتی مایکروسافت را نصب نکرده بودند، استفاده کرد و پس از ورود به سیستم، داده‌ها را رمزگذاری کرد؛ این حمله به از کار افتادن صدها هزار کامپیوتر در بیمارستان‌ها، مدارس، کسب‌وکارها و خانه‌ها در ۱۵۰ کشور منجر شد؛ سپس از قربانیان درخواست باج کرد. حمله نات‌پتیا که اعتقاد بر این است روسیه به‌عنوان بخشی از تلاش‌های خود در بی‌ثبات‌سازی اوکراین در آن دست داشته است، از طریق یک به‌روزرسانی در نرم‌افزار یک شرکت حسابداری اوکراینی اجرا شد. نات‌پتیا با حمله

---

۱. بخش‌هایی که به‌دلیل دارایی‌ها، سیستم‌ها و شبکه‌هایشان، خواه به‌صورت فیزیکی یا مجازی، برای ایالات متحده بسیار حیاتی تلقی می‌شوند، به‌طوری که نقص یا نابودی آنها اثرات مهلکی بر امنیت، اقتصاد، بهداشت یا ایمنی عمومی ملی خواهد گذاشت.

به دولت و سیستم‌های کامپیوتری اوکراین آغاز شد و به دیگر بخش‌های جهان گسترش یافت و شرکت‌هایی مانند شرکت کشتیرانی دانمارکی «مرسک»، شرکت دارویی «مرک»، شرکت تولیدکننده شکلات «کدبری» و غول تبلیغاتی «دبلیو پی پی» را آلوده کرد.

آسیب‌پذیری رو به رشد

تحول دیجیتال با رشد اتوماسیون، اینترنت اشیا، پردازش و ذخیره‌سازی ابری، هوش مصنوعی و یادگیری ماشین شتاب بیشتری می‌گیرد. گسترش و وابستگی روزافزون به فناوری‌های پیچیده، متصل به اینترنت و مبتنی بر نرم‌افزارهای دیجیتال در حوزه امنیت سایبری مشکلات جدی به وجود آورده است. در یک مقاله که در سال ۲۰۱۴ توسط مرکز امنیت نوین آمریکا منتشر شد، «ریچارد جی دانزیگ»، وزیر سابق نیروی دریایی و رئیس هیات‌مدیره این مرکز، تناقض‌های مطرح‌شده توسط فناوری‌های دیجیتال را توضیح داده است: «فناوری‌های دیجیتال در عین حال که قدرت بی‌سابقه‌ای را به ارمغان می‌آورند، امنیت کاربران را کمتر می‌کنند. قابلیت‌های ارتباطی آنها همکاری و شبکه‌سازی را امکان‌پذیر می‌کند، اما در عین حال راه را برای نفوذ هموارتر می‌سازد. متمرکزسازی داده، کارایی و مقیاس عملیات را بسیار بهبود بخشیده است، اما این متمرکزسازی به نوبه خود به‌صورت بالقوه حجم داده‌ای را که می‌تواند به‌دنبال یک حمله به سرقت رود یا تخریب شود، افزایش می‌دهد. پیچیدگی‌های سخت‌افزاری و نرم‌افزاری قابلیت‌های زیادی ایجاد می‌کند، اما این پیچیدگی‌ها نقاط آسیب‌پذیری را به وجود می‌آورند و قدرت کشف نفوذها را کاهش می‌دهند... در مجموع سیستم‌های سایبری به ما غذا می‌دهند، اما در عین حال ما را ضعیف کرده و مسموم می‌کنند.»

واقعیت این است که این فناوری‌ها به قدری پیچیده‌اند که حتی وندورهایی که آنها را ایجاد کرده و به‌خوبی می‌شناسند نیز به‌طور کامل نقاط آسیب‌پذیر آنها را درک نمی‌کنند. وندورها معمولا اتوماسیون را به‌عنوان راهی برای از بین بردن ریسک‌های ایجادشده توسط انسان‌های مستعد خطا به فروش می‌رسانند، اما این اقدام صرفا ریسک‌ها را با ریسک‌های جدید جایگزین می‌کند. در حال حاضر سیستم‌های اطلاعاتی چنان پیچیده‌اند که شرکت‌های ایالات متحده به‌طور متوسط باید بیش از ۲۰۰ روز زمان بگذارند تا تشخیص دهند که مورد رخنه سایبری قرار

گرفته‌اند. طبق گزارش موسسه «پونمون»[1]؛ مرکزی که پژوهش‌های مستقلی را در مورد حریم خصوصی، حفاظت از داده و سیاست امنیت اطلاعات انجام می‌دهد، شرکت‌ها اغلب نشت داده سیستم‌های خود را متوجه نمی‌شوند و توسط اشخاص ثالث از این موضوع مطلع می‌شوند.

با وجود گسترش تعداد حملات سایبری خسارت‌بار و شناخته‌شده در سراسر جهان علیه شرکت‌هایی چون «تارگت»، «سونی پیکچرز»، «آکوئیفاکس»، «هوم‌دیپات»، «مرسک»، «آرامکو» و... مدیران کسب‌وکارها نتوانسته‌اند در برابر وسوسه فناوری‌های جدید و مزیت‌های فراوانی که به همراه می‌آورند، مقاومت کنند؛ کارایی بیشتر، نیروی کار کمتر، کاهش یا از بین بردن خطاهای انسانی، بهبود کیفیت، ایجاد فرصت‌هایی برای کسب اطلاعات بیشتر در مورد مشتریان، توانایی ایجاد محصولات و خدمات جدید از جمله این مزیت‌ها هستند. مدیران هرساله هزینه‌های بیشتری برای فناوری‌های امنیتی جدید و استخدام مشاوران اختصاص می‌دهند، رویکردهای سنتی در زمینه امنیت سایبری را حفظ می‌کنند و به بهبود شرایط امیدوار هستند. این یک طرز تفکر خیالی است.

محدودیت‌های «بهداشت سایبری»[2]

رویکردهای سنتی در حوزه امنیت سایبری یا به عبارت دیگر بهداشت سایبری شامل موارد زیر است:

- ایجاد فهرست جامعی از دارایی‌های سخت‌افزاری و نرم‌افزاری یک شرکت؛
- خرید و به‌کارگیری جدیدترین ابزارهای سخت‌افزاری و نرم‌افزاری دفاعی، شامل امنیت نقطه پایانی[3]، فایروال‌ها و سیستم‌های تشخیص نفوذ؛
- آموزش منظم کارکنان جهت شناسایی و اجتناب از ایمیل‌های فیشینگ؛
- ایجاد «شکاف‌های هوایی»[4] (به‌صورت تئوری، جداسازی سیستم‌های حیاتی از شبکه‌های دیگر و اینترنت)، اگرچه در عمل چنین چیزی وجود ندارد؛
- ایجاد واحد امنیت سایبری بزرگی که خدمات مختلفی ارائه می‌دهد و اقدامات فوق را

1. Ponemon Institute
2. Cyber Hygiene
3. Endpoint security
4. Air gaps

نیز مدیریت می‌کند.

بسیاری از سازمان‌ها از چارچوب امنیت سایبری موسسه ملی استانداردها و فناوری (NIST) و چارچوب ۲۰ کنترل امنیتی موسسه «SANS» پیروی می‌کنند. این چارچوب‌ها مستلزم انجام پیوسته صدها فعالیت هستند که شامل الزام کارکنان به استفاده از رمز عبورهای پیچیده و تغییر مداوم آنها، رمزگذاری داده‌ها هنگام انتقال، تقسیم‌بندی شبکه‌ها با قرار دادن فایروال بین آنها، نصب فوری پچ‌های امنیتی جدید، محدود کردن تعداد افرادی که به سیستم‌های حساس دسترسی دارند، بررسی دقیق تامین‌کنندگان و... می‌شود.

به نظر می‌رسد بسیاری از مدیرعاملان اعتقاد دارند که با پیروی از رویه‌های بهداشت سایبری، می‌توانند از سازمان خود در برابر آسیب‌های سهمگین محافظت کنند. بسیاری از نشت‌های داده شناخته‌شده، غلط‌بودن این فرضیه را به‌وضوح نشان می‌دهند. تمام شرکت‌هایی که پیش‌تر ذکر شد، از واحد امنیت سایبری بزرگی برخوردار بودند و پس از اینکه متحمل نشت داده شدند، مبالغ قابل توجهی را در امنیت سایبری هزینه کردند. بهداشت سایبری در مقابل ابزارهای خودکار معمولی و هکرهای تازه‌وارد کارآمد است، اما در مورد شناسایی تعداد رو به‌رشد تهدیدات هدفمند و پایدار هکرهای کارآزموده و حرفه‌ای علیه دارایی‌های حیاتی کارایی ندارد.

در صنایع دارایی‌محوری چون انرژی، حمل‌ونقل و تولید تجهیزات سنگین، هیچ میزانی از تخصص یا پول نمی‌تواند تمام موارد ارائه‌شده در رعایت بهداشت سایبری را بدون خطا انجام دهد. در واقع، بسیاری از سازمان‌ها در همان گام اول، یعنی ایجاد فهرست جامعی از دارایی‌های سخت‌افزاری و نرم‌افزاری یک شرکت با شکست مواجه می‌شوند. این یک ضعف بزرگ است، چون شما نمی‌توانید چیزی را که حتی از آن اطلاعی ندارید، ایمن کنید.

بنابراین در پیش گرفتن اصول بهداشت سایبری، ماهیتی بینابینی دارند. برای نصب به‌روزرسانی‌های امنیتی معمولا باید سیستم‌ها خاموش شوند، اما این کار همیشه امکان‌پذیر نیست. برای مثال، شرکت‌های خدماتی، شیمیایی و دیگر شرکت‌هایی که بر قابلیت دسترسی و اطمینان فرایندها یا سیستم‌های صنعتی خود بسیار تاکید می‌کنند، نمی‌توانند سیستم‌هایشان را هر زمانی که یک شرکت نرم‌افزاری پچ امنیتی جدید منتشر کرد، متوقف کنند؛ بنابراین آنها تمایل دارند که پچ‌های امنیتی جدید را هر چند وقت یک بار به‌صورت یکجا در زمان خاموشی

برنامه‌ریزی‌شـــده نصب کنند که این زمان معمولا چند ماه پس از انتشار یک پچ است. مساله دیگر حفاظت از دارایی‌های پراکنده است. شرکت‌های خدماتی بزرگ هزاران ایستگاه فرعی که اغلب تا صدها مایل دورتر گســـترش یافته‌اند را اداره می‌کنند. بنابراین به‌روزرســـانی این سیستم‌های پراکنده کار طاقت‌فرسایی است؛ اگر می‌توانید به نرم‌افزار از طریق شبکه دسترسی پیدا کنید تا به‌روزرسانی را انجام دهید، یک هکر مستعد ممکن است به همین روش به شبکه نفوذ و به نرم‌افزار دسترسی یابد و برای اهداف شـــرورانه از آن استفاده کند، اما اگر کارکنان‌تان نرم‌افزار را در همه نقاط به‌صورت فیزیکی به‌روز کنند، این اقدام می‌تواند بسیار هزینه‌بر باشد و اگر شما این کار را در قالب یک قرارداد به شرکت دیگری واگذار کنید، نمی‌توانید امیدوار باشید که کاملا درست انجام می‌شود.

حتی اگر ایـــن رویه‌های امنیتـــی اعم از به‌روزرســـانی‌های مداوم و... به‌طـــور کامل قابل پیاده‌سازی باشند، باز هم از پس هکرهای کارآزموده‌ای که کاملا مجهز، صبور و دائما در حال تحول هستند و همیشه می‌توانند روزنه‌هایی برای عبور پیدا کنند، برنخواهند آمد. مهم نیست که بهداشت سایبری شرکت شما تا چه اندازه خوب باشد، زیرا یک حمله هدفمند از شبکه‌ها و سیستم‌های شما عبور خواهد کرد. ممکن اســـت این کار برای هکرها هفته‌ها یا ماه‌ها طول بکشد، اما در هر صورت آنها وارد خواهند شد.

این فقط نظر من نیست. «مایکل آسانته»، مدیر امنیتی ارشد سابق «آمریکن الکتریک‌پاور» و یکی از رهبران فعلی موسسه «SANS» به من گفت: «بهداشت سایبری برای دفع حملات جوجه‌هکرها مناسب است» و «در صورتی که در یک دنیای آرمانی به‌خوبی انجام شود، ممکن است ۹۵ درصد از مهاجمان را ناکام کند»؛ اما او می‌گوید در دنیای واقعی، بهداشت سایبری «تنها به مانند یک سرعت‌گیر در مسیر رسیدن مهاجمان کارآزموده به یک هدف خاص» عمل می‌کند. «باب لرد»، رئیس سابق امنیت یاهو و توییتر، در مصاحبه‌ای با روزنامه «وال‌استریت ژورنال» در سال گذشـــته اظهار داشـــت که «وقتی با مدیران امنیتی شرکت صحبت می‌کنم، این گزاره که ناشی از مقداری جبرگرایی اســـت را می‌شنوم که من نمی‌توانم در مقابل حملات فوق‌العاده پیچیده که توسط دولت‌ها پشتیبانی می‌شـــود، دفاع کنم؛ بنابراین، این یک بازی از پیش باخته است. پس در واقع دیگر نمی‌خواهم در مورد این مشکل عمیقا فکر کنم».

یک مورد قابل توجه حمله ویروس شامون[1] در سال ۲۰۱۲ به تاسیسات نفتی شرکت آرامکو عربستان سعودی بود که در آن زمان نسبتا دفاع قابل قبولی در برابر آن انجام شد. این حمله که مقامات آمریکایی این احتمال را می دهند که توسط ایران سازمان‌دهی شده باشد اطلاعات سه چهارم رایانه‌های این شرکت نفتی را پاک کرد. حمله‌ای دیگر در ماه مارس سال ۲۰۱۸ انجام شد و هدف آن ایجاد انفجار در یک کارخانه پتروشیمی متعلق به عربستان سعودی با نفوذ به سیستم‌های کنترل کننده امنیتی بود. بر اساس گزارش نیویورک‌تایمز اگر در طرح مهاجمان هیچ خطایی وجود نداشت، ممکن بود با موفقیت به سرانجام برسد. مهاجمان نه تنها باید راه نفوذ به سیستم را پیدا می‌کردند بلکه باید از نحوه طراحی کارخانه نیز حد قابل قبولی آگاهی می‌داشتند تا بتوانند تشخیص دهند کدام لوله‌ها به کجا منتهی می‌شوند و کدام دریچه می‌تواند نقش یک ماشه را برای انفجار ایفا کند.

ایده رادیکال INL

اکنون زمانی است که یک رویکرد کاملا متفاوت را پذیرا باشیم؛ یک تغییر کاملا انتخابی از اتکای کامل به پیچیدگی‌ها و ارتباطات دیجیتال. این اقدام می‌تواند با شناسایی اساسی‌ترین فرایندها و کارکردها و سپس کاهش یا از بین بردن مسیرهای دیجیتالی که مهاجمان می‌توانند از آن برای دستیابی به آنها استفاده کنند، صورت گیرد.

INL یک رویکرد گام‌به‌گام به نام روش مهندسی سایبری آگاهانه پیامدمحور (CCE) را توسعه داده است. هدف CCE یک ارزیابی ریسک تک‌مرحله‌ای نیست؛ بلکه هدف، تغییر دائمی این موضوع است که رهبران ارشد در مورد ریسک‌های سایبری استراتژیک پیش روی شرکت‌های خود چگونه فکر می‌کنند و آن را چگونه ارزیابی می‌کنند. اگرچه این رویکرد هنوز در مرحله مقدماتی است، ولی شاهد نتایج خوبی بودیم و این برنامه را داریم که در سال ۲۰۱۹، CCE را کاملا گسترش دهیم و تا سال ۲۰۲۰ به شرکت‌های خدماتی متعددی مجوز پیاده‌سازی این روش را ارائه بدهیم؛ اما حتی هم‌اکنون نیز مبانی اصلی رویکرد CCE می‌تواند توسط هر سازمانی به کار گرفته شود (این آزمایشگاه یک چارچوب مکمل را نیز توسعه داده است؛ مهندسی سایبری اگاهانه {CIE} که در بسیاری از جنبه‌ها مشابه CCE است و

1. Shamoon

روش‌هایی برای کاهش یکپارچه ریسک سایبری در تمام چرخه عمر مهندسی ترسیم می‌کند).

این روش شامل چهار مرحله است که باید توسط افراد زیر طبق یک شیوه کاملا مشارکتی انجام شود:

- یک استاد CCE که در حال حاضر یکی از کارکنان INL است، اما در آینده افرادی هستند که توسط INL آموزش دیده‌اند.
- تمام مدیرانی که در زمینه تطبیق با رگولاتوری، امور حقوقی و کاهش ریسک مسئولیت دارند؛ شامل مدیرعامل، مدیر ارشد عملیاتی، مدیر ارشد مالی، مدیر ارشد ریسک، مشاور کل و مدیر ارشد امنیت.
- افرادی که بر کارکردهای عملیاتی اصلی نظارت دارند.
- کارشناسان سیستم امنیتی، اپراتورها و مهندسانی که آشنایی بیشتری با فرایندهای حیاتی شرکت دارند.
- کارشناسان سایبری و مهندسان فرایندی که می‌دانند چگونه سیستم‌ها و تجهیزات ممکن است مورد سوءاستفاده قرار گیرند.

برای بعضی از این افراد، این فرایند پراسترس خواهد بود. برای مثال، افشای ریسک‌های سازمانی که تاکنون ناشناخته مانده است به احتمال زیاد مدیر ارشد امنیت را خجالت‌زده خواهد کرد؛ اما این موضوع در بسیاری از موارد عادلانه نیست. هیچ مدیر ارشد امنیتی نمی‌تواند شرکتی را در برابر یک حمله صورت‌گرفته توسط یک مهاجم بسیار مجهز کاملا آماده کند.

۱. شناسایی فرایندهای «تاج جواهرنشان»[1]

کار با آنچه INL آن را اولویت‌بندی پیامدها می‌نامد، آغاز می‌شود؛ ایجاد سناریوهایی فاجعه‌بار یا رویدادهایی با پیامدهای احتمالی بسیار. این اقدام شامل شناسایی کارکردها و فرایندهایی است که نقص در آنها به‌قدری خسارت‌بار خواهد بود که می‌تواند بقای یک شرکت را تهدید کند. یکی از نمونه‌ها شامل حمله به ترانسفورماتورهاست که می‌تواند به مدت یک ماه عملیات توزیع برق یک شرکت خدمات الکتریکی را متوقف سازد (یا حمله به ایستگاه‌های افزایش فشار که می‌تواند مانع عملیات گازرسانی یک شرکت توزیع گاز طبیعی به مشتریان

1. crown jewel

خود شود). دیگر نمونه‌ها شـــامل یک حمله هدفمند به سیســـتم‌های امنیتی در یک کارخانه تولید محصولات شیمیایی یا یک پالایشگاه نفت اســـت که می‌تواند به انفجاری بینجامد که باعث مرگ یا مصدومیت صدها یا هزاران نفر شـــود و در پی آن دعاوی حقوقی به‌دنبال وقوع خسارت‌های ویرانگر مطرح شـــود، ارزش بازار شرکت به شدت افت کند و به قیمت از دست رفتن شغل مدیران این شرکت تمام شود.

تحلیلگران آشنا با چگونگی عملکرد مهاجمان سایبری کارآزموده در پیش‌بینی اهداف نهایی مهاجمان آتی کمک می‌کنند. با مطرح‌کردن ســـوالاتی چون «شما در صورتی که قصد داشته باشید فرایندهای شرکت را مختل یا شـــرکت خود را نابود کنید، چه کاری انجام می‌دهید؟» و «در صورتی که بخواهید به شرکت حمله سایبری انجام دهید، اولین تاسیساتی که سخت برای دســـتیابی به آن تلاش می‌کنید، چه چیزی خواهد بود؟»، تیم می‌تواند اهدافی که اختلال در آنها مخرب‌ترین و محتمل‌ترین باشد را شناســـایی کند و سناریوهایی را برای مطرح‌کردن آنها در گفت‌وگو با اعضای مدیریت عالی توسعه دهد. بسته به اندازه شرکت، این گام ممکن است هفته‌ها یا ماه‌ها طول بکشد.

۲. ترسیم زمین دیجیتال

اقدام بعدی که معمولا یک هفته کامل یا بیشـــتر طول می‌کشد، ترسیم تمام سخت‌افزارها، نرم‌افزارها، فناوری‌های ارتباطی، افراد و فناوری‌های پشتیبان (شامل تامین‌کنندگان و خدمات شخص ثالث) در سناریوهای نابودی شرکت است. این اقدام مستلزم توصیف مراحل تولید، مستندسازی تمام مکان‌هایی که سیستم‌های کنترل و اتوماسیون به کار گرفته می‌شوند و ثبت تمام ورودی‌های فیزیکی یا داده‌ای به این کارکرد یا فرایند است. این اتصالات گذرگاه‌های بالقوه مهاجمان هستند و شرکت‌ها اغلب از همه آنها آگاهی ندارند.

نقشـــه‌های موجود از این عناصر هرگز به‌طـــور کامل با واقعیت همخوانی ندارند. پاســـخ پرسش‌هایی چون «چه کسی با تجهیزات در ارتباط است؟» و «اطلاعات چگونه در شبکه‌های شما انتقال می‌یابند و شما چگونه از آنها محافظت می‌کنید؟» همواره غیر منتظره هستند. برای مثال، تیم ممکن است از گفته‌های یک معمار شبکه یا مهندس دریابد که یک سیستم حیاتی نه‌تنها به شبکه سیستم‌های عملیاتی؛ بلکه به شبکه کســـب‌وکار که با سیستم‌های پرداخت،

سیستم‌های اطلاعات مشتری و همچنین اینترنت در ارتباط است نیز متصل است. با پرسش از شخص مسئول مدیریت وندورها، تیم ممکن است مطلع شود که تامین‌کننده این سیستم به‌منظور انجام تجزیه‌وتحلیل و تشخیص از راه دور، یک اتصال بی‌سیم مستقیم را به آن برقرار می‌کند. یک تامین‌کننده سیستم امنیتی ممکن است بگوید که این نمی‌تواند به‌طور مستقیم با تجهیزات در ارتباط باشد، اما یک بررسی دقیق توسط مکانیک‌ها و به‌روزرسانی فرایندها ممکن است نشان دهد که این‌گونه نیست. هر کشفی در این مرحله یک لحظه آهان[1] برای تیم به‌دنبال دارد.

۳. مسیرهای حمله احتمالی را تبیین کنید

سپس، تیم با استفاده از یک روش توسعه‌یافته توسط «لاکهید مارتین»، کوتاه‌ترین و محتمل‌ترین مسیرهایی که مهاجمان برای دستیابی به اهداف تعیین‌شده در گام اول پیش می‌گیرند را شناسایی می‌کند. این مسیرها بر اساس میزان سختی‌شان رتبه‌بندی شده‌اند. استاد CCE و دیگر کارشناسان، شامل افرادی که به اطلاعات حساس در مورد مهاجمان و روش‌های آنها دسترسی دارند، نقش اصلی را در این مرحله ایفا می‌کنند. آنها اطلاعاتی که از منابع دولتی در مورد حمله به سیستم‌های مشابه در سراسر جهان جمع‌آوری شده را به اشتراک می‌گذارند. ورودی‌های تکمیلی شرکت در رابطه با سیستم‌های امنیتی، قابلیت‌ها و روندهای شرکت در پاسخگویی به تهدیدات سایبری و موارد دیگر، به تیم در کامل‌کردن فهرست مسیرهای حمله‌ای که در گام ۴ برای مدیران ارشد جهت اولویت‌بندی اقدامات بازسازی مورد استفاده قرار خواهد گرفت، کمک می‌کند.

۴. ایجاد گزینه‌هایی برای کاهش ریسک و محافظت در برابر آن

اکنون زمان آن رسیده که قابلیت‌هایی برای مهندسی معکوس ریسک‌های سایبری با بالاترین پیامدها را ارائه دهیم. اگر ۱۰ مسیر برای دستیابی به یک هدف وجود داشته باشد، اما همه آنها از یک نود خاص عبور کنند، بدیهی است که این نود مکانی بسیار مناسب برای نصب یک تله است، یک حسگر ردیابی دقیق که به محض دیدن اولین نشانه، به تیم «واکنش سریع مدافعان»

1. Aha moment

نسبت به وقوع یک مشکل هشدار می‌دهد.

پیاده‌سازی بعضی از اصلاحات به طرز عجیبی ساده و ارزان است؛ برای مثال، یک حسگر سیم‌پیچی‌شده و فاقد سیستم نرم‌افزاری، بخشی را که دستورالعمل‌های دیجیتالی مخربی به آن داده شده و ممکن است به آسیب‌دیدن یا نابودی آن منجر شود را کند کرده یا از کار می‌اندازد. موارد دیگر وقت و هزینه بیشتری می‌طلبند، مانند آماده نگه‌داشتن یک سیستم پشتیبانی اضافی و مواردی از این دست. اگرچه، بسیاری از اصلاحات هیچ تاثیر منفی بر کارایی عملیاتی و فرصت‌های کسب‌وکاری ندارند، اما برخی از آنها ممکن است اثرات نامطلوبی داشته باشند، بنابراین رهبران یک شرکت در نهایت باید تصمیم بگیرند که چه اقدامی برای جلوگیری، کاهش و یا انتقال ریسک‌ها انجام دهند.

اگر فرایند انتخاب‌شده یک کانال دیجیتال برای ردیابی یا ارسال سیگنال‌های کنترلی داشته باشد، هدف باید این باشد که تعداد مسیرهای دیجیتال به سمت این فرایند حیاتی در کمترین حد ممکن نگه داشته شود تا شناسایی رفت‌وآمدهای غیرعادی آسان‌تر شود. به‌علاوه، یک شرکت ممکن است دستگاهی برای محافظت از یک سیستم خریداری کند که در صورت دریافت دستورات دیجیتالی مخرب، هشدار بدهد. گاهی یک شرکت ممکن است قصد داشته باشد که افراد مورد اعتماد را به کار بگیرد تا دماسنج‌ها یا فشارسنج‌های مکانیکی را به‌عنوان مثال برای اطمینان از اینکه دستگاه‌های دیجیتال حقیقت را بیان می‌کنند، ردیابی کند. اگر شرکت شما دچار حادثه سایبری جدی نشده است، ایده جداسازی هرچه بیشتر از شبکه‌ها، نصب دستگاه‌های مکانیکی قدیمی و قرار دادن انسان‌ها در کارکردهای خودکار ممکن است مانند یک تصمیم کسب‌وکاری ضعیف در نظر گرفته شود اما در عوض باید از آن به عنوان یک تصمیم مدیریت ریسک فعال در نظر گرفته شود. این تصمیم ممکن است کارایی را کاهش دهد، اما اگر رویکردی به‌طور اساسی احتمال وقوع فاجعه‌ای را کاهش دهد که روش‌های فعلی شما نمی‌تواند از شرکت‌تان در مقابل آن محافظت کند، این رویکرد یک اقدام هوشمندانه به حساب می‌آید.

تصور اینکه مدیران عامل و مدیران اجرایی ارشد این فرایند را با شک و تردید نظاره کنند، دشوار نیست. در هر پروژه مدیریت تحول، دور کردن قلب‌ها و ذهن‌ها از ایده‌هایی که آن‌ها چندین دهه است از آنها پیروی می‌کنند، یک چالش بزرگ است. بنابراین باید منتظر

مقاومت‌هایی در برابر این رویکرد، به‌خصوص در مراحل اولیه باشید. انتشار اطلاعات زیادی در مورد شرکت شما و اعتراف به نقاط ضعفی که شما آن را نمی‌دانستید یا نمی‌خواستید در مورد آنها فکر کنید به لحاظ روانی دشوار خواهد بود. مراحل بعدی پایداری مهندسان را به چالش خواهد کشید، چون سیستم‌ها و اقدامات آنها را به‌منظور شناسایی نقاط ضعف مورد بررسی قرار خواهد داد. اطمینان حاصل کنید که اعضای تیم حتی در طول سخت‌ترین ارزیابی‌ها نیز احساس امنیت می‌کنند. در پایان، اطلاعات دقیقی در مورد رویکردهای مهاجمان و آنچه آنها می‌توانند به آن دست یابند، روشن خواهد شد. حتی مقاوم‌ترین اعضای تیم نیز وقتی ریسک‌ها و بهترین روش‌ها برای کاهش آنها را شناسایی می‌کنند از هیات مدیره درخواست خواهند کرد که اقداماتی در این زمینه انجام دهد.

کاری که امروز می‌توانید انجام دهید

یاد بگیرید که مثل مهاجمان فکر کنید. شما ممکن است تا جایی پیش بروید که یک تیم داخلی ایجاد کنید که به طور دائم برای نفوذ به سیستم‌های حیاتی شما تلاش کنند تا قدرت دفاعی شما را محک بزنند.

حتی اگر شما بتوانید سطوح بالایی از بهداشت سایبری را حفظ کنید، باید برای یک نشت داده آماده باشید. بهترین راه برای انجام این کار ایجاد یک فرهنگ امنیت سایبری مشابه آن چیزی است که در کارخانه‌های تولید محصولات شیمیایی مدرن و نیروگاه‌های هسته‌ای وجود دارد. همه کارکنان، از عالی‌رتبه‌ترین آنها گرفته تا کارمندان معمولی، باید نسبت به اهمیت واکنش سریع به یک سیستم کامپیوتری یا دستگاهی که در زمان راه‌اندازی غیرعادی عمل می‌کند، آگاه باشند: این اتفاق ممکن است ناشی از یک نقص فنی باشد، اما ممکن است نشان‌دهنده یک حمله سایبری نیز باشد.

سرانجام، هرگاه شما و تیم‌تان اعتماد خود را نسبت به سیستم‌هایی که از حیاتی‌ترین کارکردهای شما پشتیبانی می‌کنند، از دست دادید، باید برای پیاده‌سازی یک طرح جایگزین آماده باشید. این طرح باید طوری طراحی شود که به شرکت شما این امکان را بدهد که عملیات ضروری شرکت را تا حد امکان ادامه دهد. در حالت ایده‌آل، سیستم پشتیبانی باید نه به فناوری‌های دیجیتال متکی و نه به یک شبکه (به ویژه اینترنت) متصل باشد. اما دست‌کم، این

طرح نباید همان عملکردهای سیستم اصلی را تکرار کند، به یک دلیل واضح: اگر مهاجمان توانستند به سیستم اصلی نفوذ پیدا کنند، پس به آسانی قادر خواهند بود که به همین شکل به این طرح جایگزین نیز حمله کنند.

هر سازمانی که به فناوری‌های دیجیتال و اینترنت وابسته است، در مقابل یک حمله مخرب آسیب‌پذیر است. حتی بهترین بهداشت سایبری نیز قادر نخواهد بود روسیه، کره شمالی و گروه‌های جنایی و تروریستی بسیار ماهر و مجهز را متوقف سازد. تنها راه برای حفاظت از کسب‌وکارتان این است که تا جای ممکن رویکردهایی در پیش گیرید که ممکن است از نظر فناوری یک گام رو به عقب به نظر برسند اما در واقعیت یک گام هوشمند رو به جلو هستند. هدف کاهش (و حتی حذف) وابستگی کارکردهای حیاتی به فناوری‌های دیجیتال و اتصال آن‌ها به اینترنت است. این اقدامات ممکن است هزینه‌های بیشتری به ما تحمیل کند اما در مقایسه با هزینه بالقوه نابودی کسب‌وکار بر اثر حمله سایبری ناچیز است.

جمع‌بندی

فناوری‌های دیجیتال قابلیت‌ها و کارایی‌های جدیدی برای ما به ارمغان می‌آورند اما آن‌ها چالش‌های امنیتی جدیدی را نیز به دنبال دارند. اهمیتی ندارد که شرکت شما چه قدر در شیوه‌های دفاعی سنتی امنیت سایبری مانند سخت‌افزار، نرم‌افزار و آموزش سرمایه‌گذاری کند:

- اگر سیستم‌های حیاتی شرکت شما دیجیتالی و متصل به اینترنت باشند، آن‌ها هرگز نمی‌توانند به طور کامل ایمن شوند.
- حتی اگر رویه‌های بهداشت سایبری به طور کامل پیاده‌سازی شوند، هکرها آن‌قدر کارآزموده، مجهز، صبور، در حال تحول و بامهارت هستند که راهی برای ورود به سیستم پیدا کنند.
- فرآیندها یا کارکردهایی که یک نشست داده در آن‌ها می‌تواند کسب‌وکار شما را به خطر اندازد را شناسایی کنید و آن‌ها را تا جای ممکن از اینترنت جدا سازید، وابستگی آن‌ها به فناوری‌های دیجیتال را به حداقل برسانید و آن‌ها را با دستگاه‌های آنالوگ و افراد مورد اعتماد کنترل کنید.
- همه سخت‌افزارها، نرم‌افزارها و فناوری‌های ارتباطی به همراه فرآیندها و افرادی که از

آن‌ها پشتیبانی می‌کنند را در این سناریو فهرست کنید.

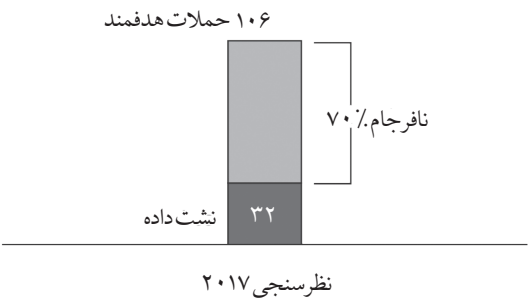
- یاد بگیرید که مثل مهاجمان فکر کنید و مسیرهای احتمالی که آنها برای دستیابی به اهداف شما دنبال می‌کنند را شناسایی کنید.
- فرهنگی ایجاد کنید که در آن همه کارکنان نسبت به بروز رفتار غیرعادی از سیستم‌های کامپیوتری یا دستگاه‌ها حساس شده و از اهمیت واکنش سریع به آن آگاه باشند.

۲. روندهای امنیتی بر اساس آمار

اسکات برناتو و مت پری

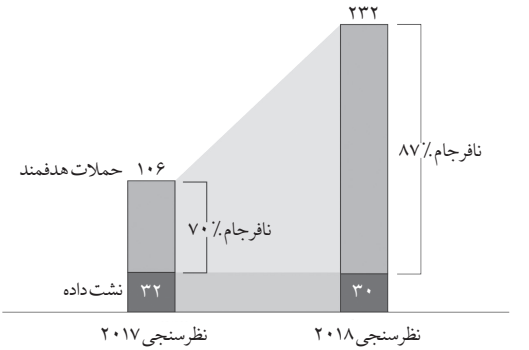
برای درک وضعیت ناامیدکننده امنیت سایبری، ابتدا به شکل ۱-۲ که برگرفته از نظرسنجی‌های انجام‌شده از شرکت‌هایی در سراسر جهان در سال ۲۰۱۷ است، توجه کنید. از پاسخ‌دهندگان در مورد وقوع حملات هدفمند، حملات با پتانسیل نفوذ به شبکه‌های دفاعی و ایجاد خسارت یا سرقت دارایی‌های ارزشمند (بدون توجه به فعالیت‌های خرابکارانه سطح پایینی که بیش از آنکه یک تهدید به حساب آیند، صرفا آزاردهنده هستند) در شرکت آنها، پرسش به عمل آمد.

همچنین آنها در خصوص حملاتی که پیش از این به نشت داده‌ها منجر شده نیز گزارشی دادند.



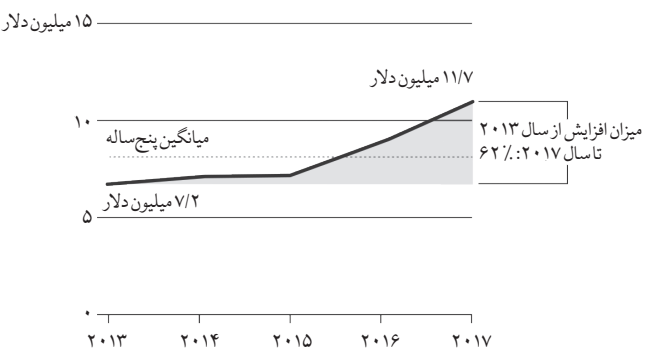
شکل ۱-۲: میانگین سالانه تعداد حملات هدفمند و نشت داده در هر شرکت. (منبع: اکسنچر)

طبق یک نظرسنجی مشابه در سال ۲۰۱۸ (شکل ۲-۲)، نسبت حملات هدفمندی که نافرجام مانده بود تا ۸۷ درصد افزایش داشت. این موضوع ممکن است خبر خوبی به نظر آید، اما تعداد حملات همچنان در حال افزایش است.



شکل ۲-۲: حتی با وجود آنکه ما بسیاری از حملات را خنثی ساختیم، ولی از بیشتر نشت داده‌ها نتوانستیم جلوگیری کنیم. (منبع: اکسنچر)

با در نظر گرفتن داده‌های شکل ۳-۲ این مساله روشن می‌شود که شرکت‌ها پیشرفتی در این زمینه نداشته‌اند. شرکت‌ها تقریبا به‌طور میانگین به اندازه حملاتی که صورت می‌گیرد، شاهد نشت داده هستند. کارشناسان معتقدند که این تعداد به‌صورت قابل توجهی کاهش نخواهد داشت، چون حملات در حال افزایش هستند. به علاوه، آنها نگران این موضوع هستند که نشت داده‌ها سازمان‌های مهم‌تری را هدف قرار دهند و عواقب گسترده‌تری به همراه داشته باشند. تشدید اقدامات پیشگیرانه و افزایش خسارات مالی که یک نشت داده به شرکت تحمیل می‌کند، هزینه شرکت‌ها را در مواجهه با موضوع امنیت سایبری بالا می‌برد.



شکل ۳-۲: میانگین هزینه جرائم سایبری برای هر شرکت (بر مبنای دلار آمریکا). (منبع: اکسنچر و پونمون)

در این فصل وضعیت امنیت سایبری را با نمودارهای برگرفته از سه گزارش بسیار معتبر بررسی می‌کنیم. «گزارش تحقیقات صورت‌گرفته در مورد نشت داده‌ها در سال ۲۰۱۸» وریزون[1] که بیش از ۵۳ هزار حادثه امنیت سایبری (حوادثی که به‌طور بالقوه داده‌ها را افشا می‌کند) و ۲۲۱۶ مورد نشت اطلاعاتی (حوادثی که منجر به افشای داده‌ها می‌شود) در ۶۵ کشور را تجزیه‌وتحلیل کرده است. گزارش «وضعیت تاب‌آوری سایبری در سال ۲۰۱۸» اکسنچر که بر مبنای نظرسنجی‌های انجام‌گرفته از ۴۶۰۰ مدیر اجرایی در شـــرکت‌هایی با ارزش بیش از یـــک میلیارد دلار در ۱۹ صنعت در میان ۱۵ کشور است. گزارش «بررسی هزینه جرائم سایبری ۲۰۱۷» اکسنچر که با همکاری موسسه «پونمون» تهیه شده و الهام‌گرفته از پاسخ‌های ۲۵۴ شرکت در هفت کشور است. اگرچه دســـتیابی به داده‌های معتبر و قطعی در خصوص حوادث امنیت سایبری دشوار است، اما این گزارش‌ها در کنار یکدیگر تصویر نسبتا دقیقی از وضعیت امنیت سایبری را فراهم می‌کنند. داده‌های به دست آمده از این گزارش‌ها یک واقعیت دوگانه را نشان می‌دهند. از یک سو کلیت حملات تغییری نداشته‌اند؛ حملات به‌صورت مداوم اتفاق می‌افتند و بسیاری از آنها همان ترفندهای فنی که سال‌هاست استفاده می‌شود را به کار می‌گیرند. از سویی دیگر، حملات به‌صورت رادیکالی تغییر کرده‌اند؛ در حال حاضر تعداد حملات بیشتر از هر زمان دیگری است و اثرات منفی بیشتری نیز به دنبال دارد. ما شاهد حملات بیشتری به زیرساخت‌های حیاتی هستیم و «باج‌افزارها» که کاربران را از داده‌ها یا ابزارهای دیجیتالی خود تا زمانی که مبلغی به‌عنوان باج پرداخت نکنند، محروم می‌سازند نیز رشد قابل ملاحظه‌ای داشـــته‌اند. در اینجا آن چیزی که امروزه در مورد امنیت سایبری می‌دانیم، آورده شده است.

چه کسانی وارد می‌شوند؟

تقریبا یک‌چهارم موارد نشت اطلاعات، از منابع داخلی ناشی می‌شود، اما بیشتر صنایع نسبت به میانگین، انحراف دارند (شکل ۴-۲). نسبت خرابکاران داخلی در حوزه‌هایی که اطلاعات بسیار حساس و ارزشمندی دارند (مراقبت‌های بهداشتی، مدیریت عمومی و خدمات حرفه‌ای، فنی و علمی) بالاتر است، این در حالی است که صنایعی که به‌طور مستقیم با مردم سروکار دارند

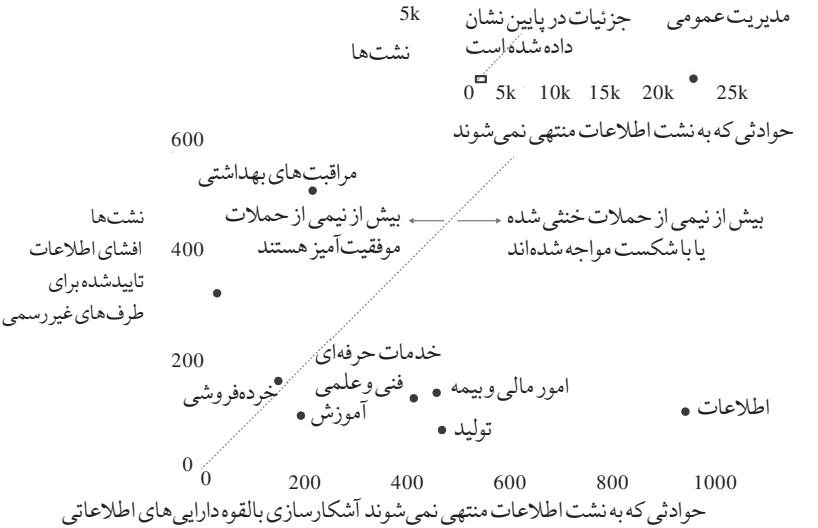
1. Verizon

(مانند رستوران‌ها و فروشگاه‌ها بیشتر) از منشاء خارجی مورد حمله قرار می‌گیرند.

شکل ۴-۲: اغلب حملات از منشاء خارجی ناشی می‌شوند.

هکرها چند بار وارد می‌شوند؟

هکرها در تعداد اندکی از صنایع به‌شدت آسیب‌پذیر غالبا نفوذ می‌کنند، اما در بیشتر موارد، برای موفق‌شدن باید حملات متعددی صورت گیرد.

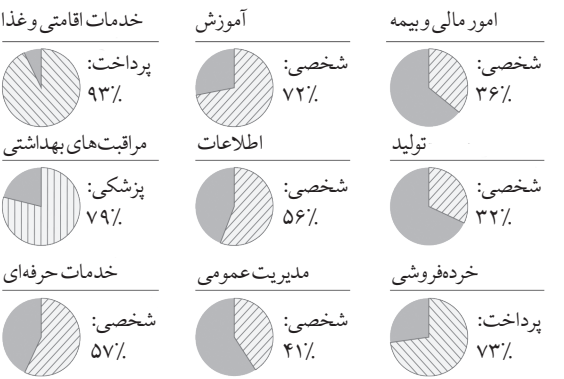


شکل ۵-۲: حملات همچنان بیشتر به شکست منتهی می‌شوند تا موفقیت. (منبع: وریزون)

نسبت حوادث منجر به نشت اطلاعات در یک صنعت بیانگر میزان آسیب‌پذیری آن است. خدمات اقامت و صنایع غذایی یکی از آسیب‌پذیرترین بخش‌ها هستند؛ این بخش‌ها به‌طور میانگین به ازای هر حمله ناموفق ۱۱ نشت اطلاعات به‌دنبال دارد، اگرچه هزینه جبران این نفوذها در این بخش نسبت به سایر صنایع پایین‌تر است. بخش عمومی در معرض حملات گسترده‌ای است که بیشترین تعداد حوادث رخ‌داده در صنایع مورد مطالعه را شامل می‌شود، البته بیشتر آنها با شکست مواجه می‌شوند؛ به ازای هر ۷۴ حمله ناموفق، یک نشت اطلاعات در این بخش صورت می‌گیرد.

هکرها چه چیزی به دست می‌آورند؟

با وجود همه تلاش‌های صورت‌گرفته در مورد حفاظت از داده‌های کاربران و کارت‌های اعتباری در سال‌های اخیر، مواردی که در شکل ۶-۲ آمده، متداول‌ترین دارایی‌های به‌سرقت‌رفته هستند. سایر اهداف مبتنی بر اطلاعات مانند قراردادها، RFPها (درخواست طرح‌های پیشنهادی) و سیستم‌های کنترلی که در اینجا به آنها اشاره نشده است، نسبت به گذشته نشت‌های بیشتری را تجربه کرده‌اند. با این حال داده‌های کاربران و کارت‌های اعتباری همچنان محبوب‌ترین و آسیب‌پذیرترین اهداف هستند که نشان می‌دهد شیوه‌های دفاعی ما به اندازه کافی کمک‌کننده نبوده است.



شکل ۶-۲: اطلاعات شخصی و اطلاعات پرداخت رایج‌ترین اهداف در معرض خطر هستند.

صنایعی که در آن نشت‌ها اکثرا نوع خاصی از اطلاعات (پزشکی، خدمات اقامتی و غذا) را شامل می‌شوند، می‌توانند در شیوه‌های دفاعی خود مهارت پیدا کنند، چون برای آنها ریسک کاملا تعریف شده است.

افراد شرور تقریبا همیشه یک شیوه را به کار می‌گیرند، اما صنایعی که اهداف متعددی دارند و هیچ‌یک از این اهداف جزء موارد بسیار در معرض خطر به‌شمار نمی‌روند (امور مالی، تولید) نیاز به یک استراتژی کاهش ریسک انعطاف‌پذیرتری دارند که آنها را برای مبارزه در چندین جبهه تجهیز کند.

صنایع مختلف گذرگاه‌های متفاوتی دارند که از طریق آنها دشمنان می‌توانند به شبکه‌ها وارد شوند، اما به این نکته هم باید توجه کرد که وب اپلیکیشن‌ها هرچند وقت یک‌بار گرفتار حملات موفق می‌شوند (شکل ۷-۲). با نگاهی به سه منبع اصلی حوادث صنعتی (در شکل به‌صورت بولت مشخص شده است) در مقابل سه منبع اصلی نشت (در شکل به‌صورت بولد و مشکی مشخص شده است) به دو نکته پی می‌بریم:

۱. اگر منشاء اصلی حوادث (incidents) و نشت‌ها (breaches) یکی باشد، آن موارد به‌شدت در معرض خطر هستند و شرکت‌ها به این موضوع آگاهی دارند، اما عاملان خرابکاری در هر صورت موفق می‌شوند. در این‌گونه مواقع به‌اصطلاح «یک جای کار می‌لنگد».

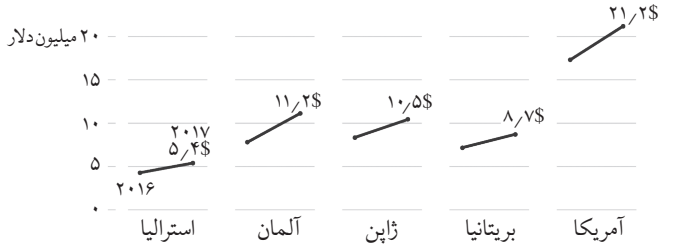
۲. اگر منشاء اصلی حوادث و نشت‌ها متفاوت باشد، شرکت‌ها در برخی جبهه‌ها در دفاع‌کردن مهارت پیدا کرده‌اند (جاهایی که تعداد حوادث بیشتر از نشت‌هاست)، اما در بعضی دیگر نقاط کوری دارند (جاهایی که تعداد نشت‌ها بیشتر از حوادث است).

منشاء اصلی نشت‌ها به‌صورت بولد و مشکی مشخص شـــده است؛ منشاء اصلی حوادث به‌صورت بولت(■) مشخص شده است.

شکل ۷-۲ : اهدافی که هکرها اغلب به آنها حمله می‌کنند و اهدافی که حمله به آنها اغلب موفقیت‌آمیز است، همیشه یکسان نیست.

چهار روش برای بررسی هزینه‌ها

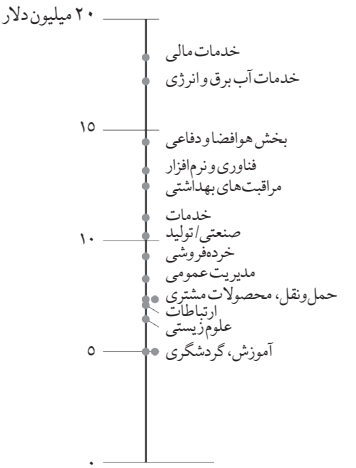
ساده‌ترین راه بررسی هزینه‌ها توجه به این نکته است که آنها، خواه از طریق سرمایه‌گذاری در شیوه‌های دفاعی و خواه با صرف هزینه جهت بازیابی اطلاعات پس از وقوع نشت‌ها، همیشه در حال افزایش هستند (شکل ۸-۲).



شکل ۸-۲: میانگین هزینه هر شرکت برای جرائم سایبری در کشورهای منتخب (بر مبنای دلار ایالات متحده)

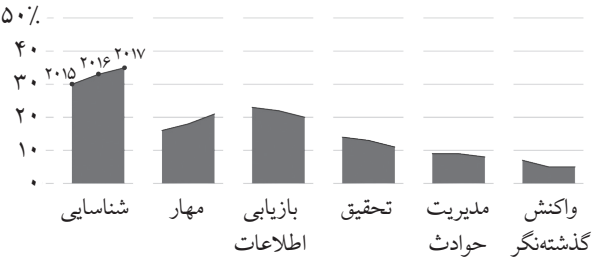
جای تعجب ندارد که هزینه جرائم سایبری در سراسر جهان در حال افزایش است. افزایش شیب هزینه‌ها نسبت به سال قبل در آلمان و ایالات متحده نشان می‌دهد که این کشورها (برای هکرها) جذاب‌ترین مقاصد هستند که ترکیبی از ارزش و آسیب‌پذیری بالا را در خود دارند.

با بررسی هزینه‌ها در هر بخش، متوجه چند نکته می‌شویم (شکل ۹-۲). هزینه جرائم سایبری برای شرکت‌های ارائه‌دهنده خدمات آب، برق، گاز و انرژی به‌دلیل وضعیت خاص این صنعت تا حدی زیاد است؛ یک نشت می‌تواند پیامدهای زودهنگام و به‌طور بالقوه مرگباری را به‌دنبال داشته باشد. هزینه‌های بخش عمومی نسبتا پایین است، اما حجم بالای حملات بدان معناست که این هزینه‌ها، به‌ویژه با افزایش اعمال خرابکارانه در سطح ایالتی، احتمالا به‌طور قابل توجهی افزایش می‌یابد.

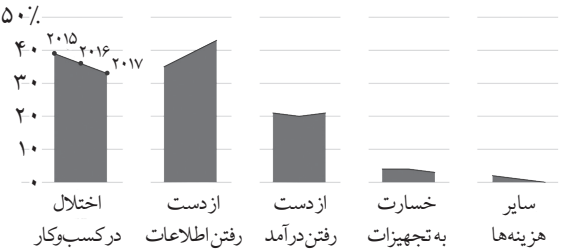


شکل ۹-۲: میانگین هزینه سالانه جرائم سایبری در هر بخش در سراسر جهان (بر مبنای دلار ایالات متحده)

همان‌طور که در شکل ۱۰-۲ نشـــان داده شده است، از ســـال ۲۰۱۵ تا ۲۰۱۷، هزینه‌های شناسایی و مهار حملات حدود پنج درصد افزایش پیدا کرده و نرخ پیشگیری از نشت اطلاعات بهبود یافته است، اما با توجه به شکل ۱۱-۲، میزان از دست رفتن درآمدها به تناسب کاهش پیدا نکرده است.



شکل ۱۰-۲: سهم هزینه‌ها در هر نوع فعالیت



شکل ۱۱-۲: سهم هزینه‌ها در پیامدهای ناشی از حمله

در حال حاضر هزینه اختلال در کســـب‌وکارها کمتر از گذشته اســـت. ما به لحاظ سرعت واکنش‌هایمان، بر خلاف روند یکنواخت حملات، در حال بهتر شدن هستیم. اما هزینه از دست رفتن اطلاعات به‌شدت افزایش یافته است. این پارادوکس بزرگ امنیت سایبری است، هرچند ما توانایی خود در خنثی کردن حملات را بهبود بخشیده‌ایم، اما سرعت وقوع حملات موفقیت‌آمیز، میزان خسارت و هزینه‌های مرتبط با آن کاهش پیدا نکرده است.

با توجه به همه این موارد، شـــرکت‌ها باید بررسی کنند که آیا ســـود حاصل از داشتن چندین سیستم آنلاین ارزش ریسک کردن دارد یا خیر. یک مکتب فکری جدید می‌گوید وقت آن است

که سیستم‌های حیاتی که وقوع نشت اطلاعاتی در آنها می‌تواند عواقب وحشتناکی داشته باشند را از کار بیندازیم. بله، شرکت‌ها بهای این کار را برای بهره‌مندی از راحتی و کارایی پرداخت خواهند کرد، اما آیا این هزینه از هزینه روزافزون خنثی‌سازی حملات فراتر نخواهد رفت؟

جمع‌بندی

وضعیت امنیت سایبری بسیار ناامیدکننده است. مجموعه نمودارهایی که با استفاده از داده‌های برگرفته از سه گزارش صنعتی بسیار معتبر طراحی شده‌اند، نشان می‌دهد که تصویر کلی این حوزه تا چه میزان ناراحت‌کننده است:

- سیستم‌هایی که دائما در معرض حملات هکرها هستند، همان رویکردهای فنی که سال‌ها مورد استفاده قرار داده‌اند را به کار می‌گیرند.
- سازمان‌هایی که اغلب حملات را خنثی می‌کنند، در حال حاضر نسبت به قبل حملات بیشتری (و خرابکارانه‌تری) به آنها تحمیل می‌شود.
- چیزی که ما در مورد حملات می‌دانیم این است که بیشتر آنها همچنان از منابع خارجی نشات می‌گیرند؛ بیش از آنکه با موفقیت همراه شوند، با شکست مواجه می‌شوند؛ متداول‌ترین اهداف‌شان، اطلاعات شخصی و اطلاعات پرداخت است.

۳. چرا هیات‌مدیره به تهدیدات سایبری رسیدگی نمی‌کند؟

یو جود چنگ[1] و بوریس گرویسبرگ[2]

یکی از بزرگ‌ترین چالش‌هایی که اعضای هیات‌مدیره با آن مواجه هستند، مساله‌ای است که مدیران نسبت به آن کمترین آمادگی را دارند؛ یعنی امنیت سایبری. در پژوهش‌هایی که پیش از این صورت گرفته است، متوجه شدیم که از نظر مدیران شرکتی که صرفا با محیط اقتصادی و رگولاتوری سروکار دارند، امنیت سایبری به‌عنوان یکی از مهم‌ترین مسائل در نظر گرفته می‌شود. مدیران، امنیت سایبری را به‌عنوان یک مساله جهانی ضروری تایید می‌کنند، اما در برقراری ارتباط میان فراگیری تهدیدات سایبری و آسیب‌پذیری شرکت‌های خود با مشکل مواجه‌اند؛ هنگامی که از آنها در مورد توصیف سطح نگرانی و آمادگی‌شان در برابر ریسک‌های مختلفی که شرکت‌شان با آن مواجه است، پرس‌وجو کردیم، امنیت سایبری در میان نگرانی‌های مربوط به ریسک‌های رگولاتوری و اعتبار از درجه اهمیت کمتری برخوردار بود. فقط ۳۸ درصد از مدیران اظهار داشتند که در مورد ریسک‌های امنیت سایبری نگرانی زیادی دارند و درصد کمی از آنها بیان داشتند که برای این ریسک‌ها آماده شده‌اند (شکل ۱-۳). به گفته یکی از این مدیران؛ «امنیت سایبری مساله بزرگی است، اما در این کسب‌وکار طیف گسترده‌ای از ریسک‌ها وجود دارد که باید مورد توجه قرار گیرد.»

وقتی مدیران، عواملی را که می‌تواند توانایی شرکت‌شان در دستیابی به اهداف استراتژیک خود را محدود کند، ارزیابی کردند، موضوع امنیت سایبری تحت‌الشعاع نگرانی‌های بارزی مانند جذب و حفظ استعدادهای برتر، محیط رگولاتوری و تهدیدات رقابت جهانی قرار گرفت (شکل ۲-۳).

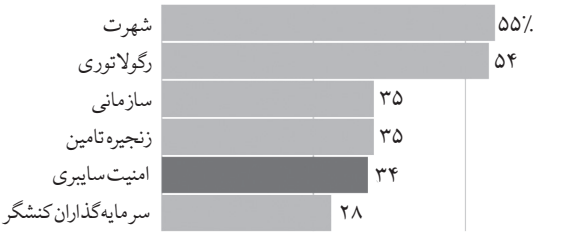
این یافته‌ها تایید می‌کند که مدیران آسیب‌های گسترده و طولانی‌مدت حمله‌ای که ممکن

1. Yo-Jud Cheng
2. Boris Groysberg

است به سازمان‌شان تحمیل شود را جدی نمی‌گیرند. با استفاده از نتایج نظرسنجی جامعی که موسسات «Women Corporate Directors» و «اسپنسر استوارت»[1] با همکاری «دبورا بل»[2]، پژوهشگر مستقل انجام دادند و از بیش از پنج‌هزار مدیر در بیش از ۶۰ کشور جهان سوالاتی در این زمینه پرسیدند، ما برای این موضوع یک دلیل عمده پیدا کردیم؛ هیات‌مدیره فاقد روال‌های مشخص و تخصص لازم برای تشخیص، ارزیابی و رسیدگی به تهدیدات سایبری است.

سوال: سطح نگرانی‌تان در حوزه‌های دارای ریسک زیر چقدر است؟

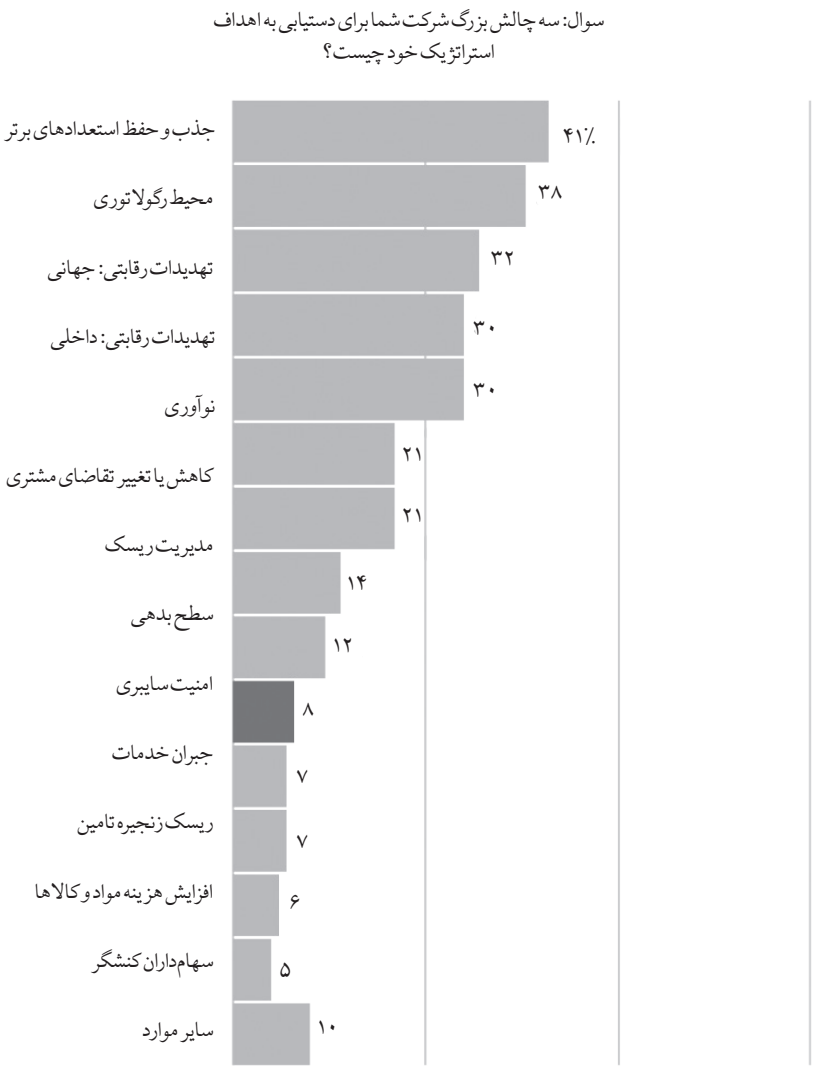
سوال: سطح آمادگی‌تان در حوزه‌های دارای ریسک زیر چقدر است؟



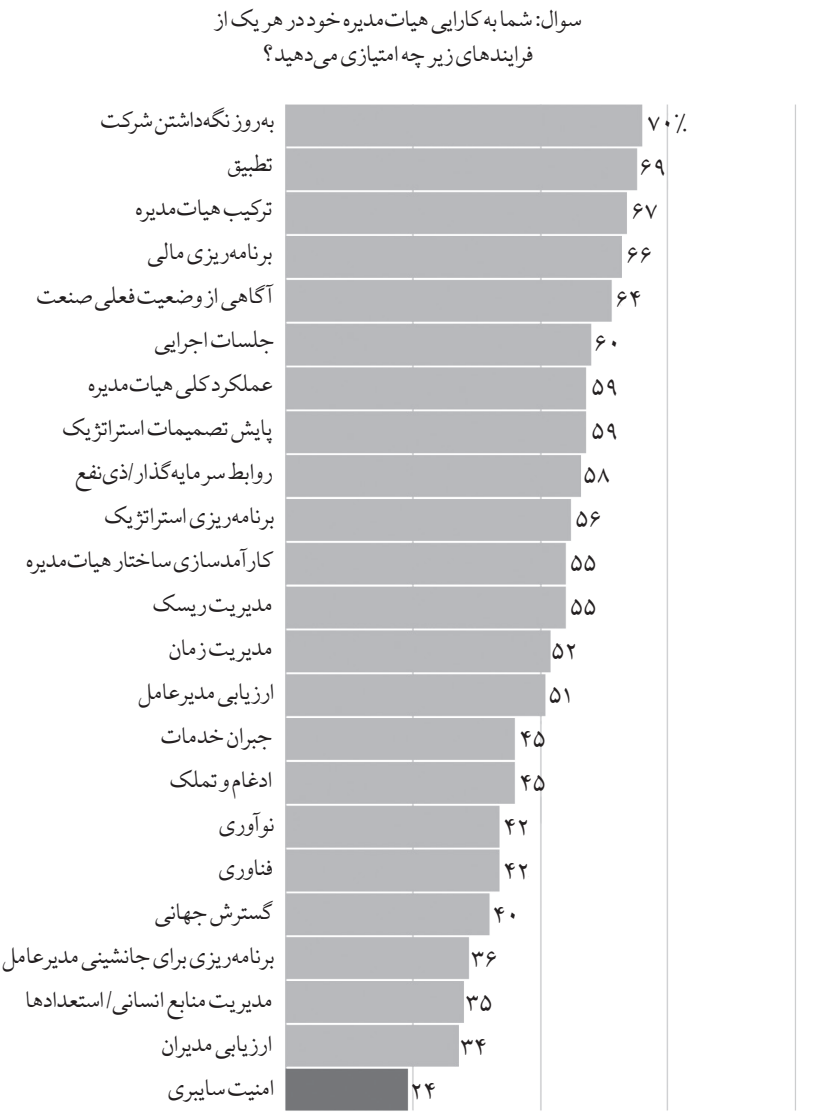
تعداد مشارکت‌کنندگان: ۳۴۰

شکل ۱-۳: اغلب اعضای هیات‌مدیره نگرانی زیاد یا آمادگی قابل قبولی برای تهدیدات سایبری ندارند.

1. Spencer Stuart
2. Deborah Bell



شکل ۲-۳: تعداد کمی از اعضای هیات‌مدیره، امنیت سایبری را به‌عنوان یک تهدید استراتژیک تلقی می‌کنند.



شکل ۳-۳: طبق نظر مدیران، اغلب فرایندهای امنیت سایبری هیات‌مدیره، ناکافی هستند.

فرایندهای ناکافی

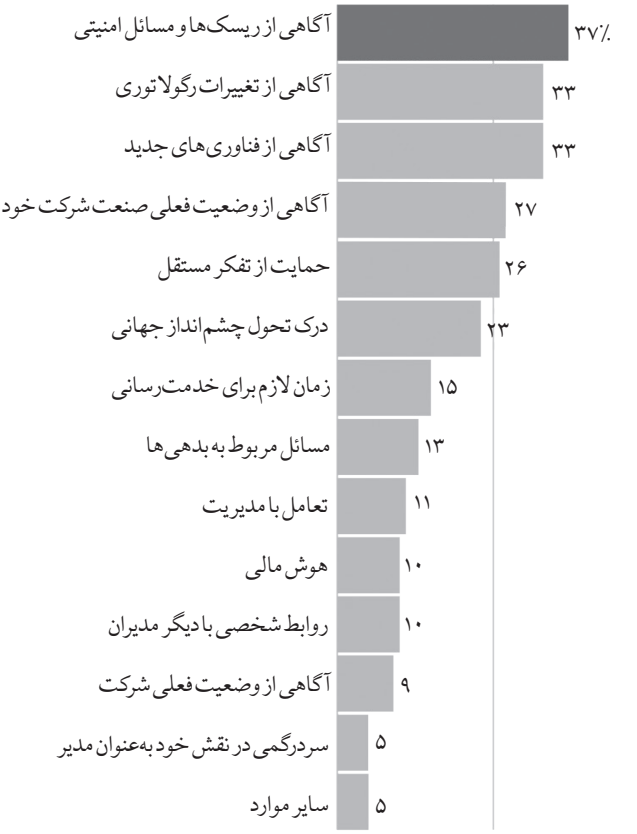
اغلب هیات‌مدیره‌ها دارای فرایندهای قوی برای رسیدگی به مسئولیت‌های بسیار ضروری خود، مانند برنامه‌ریزی مالی و انطباق با قوانین هستند؛ اما وقتی از مدیران به‌طور ویژه در مورد فرایندهای مرتبط با مسائل امنیت سایبری مانند بحث و تبادل نظر مستمر در مورد ریسک‌های سایبری (با حضور یا بدون حضور کارشناسان امنیت سایبری) و نقد و ارزیابی برنامه‌های احتمالی پس از وقوع یک نشت داده سوال کردیم، آنها به هیات‌مدیره‌های خود امتیاز پایینی دادند (شکل ۳-۳)؛ تنها ۲۴ درصد از آن فرایندها امتیاز «بالاتر از متوسط» و «عالی» دریافت کردند.

در واقع، از میان ۲۳ فرایندی که در مورد آنها سوال کردیم، مدیران پایین‌ترین امتیاز را به فرایندهای امنیت سایبری دادند.

همچنین قدرت این فرایندها در هر صنعت متفاوت است؛ هیات‌مدیره بخش‌های فناوری اطلاعات و مخابرات که ۴۲ درصد از آنها انجام اقداماتی قوی را گزارش کردند، در رده‌های نخست قرار گرفتند و در مقابل کمتر از یک‌پنجم مدیران بخش‌های مواد و صنایع چنین چیزی را عنوان کردند. در صنعت بهداشت و درمان که یک هدف متداول برای نشت داده است و اثبات شده که بسیار آسیب‌پذیر هستند، ۷۹ درصد از پاسخ‌دهندگان اظهار داشتند که سازمان‌شان فاقد فرایندهای امنیت سایبری قوی است.

فقدان تخصص

وقتی از مدیران در مورد چالش‌هایی که هیات‌مدیره با آن مواجه است، سوال شد، مسائل مرتبط با ریسک و امنیت اغلب موضوعاتی چالش‌برانگیز بودند (شکل ۴-۳). مدیران اظهار داشتند که مشکل اصلی در واقع این بود که اعضای هیات‌مدیره فاقد تخصص کافی بودند. یکی از مدیران به موضوع «عدم درک مساله و نبود اشتیاق به‌منظور ایجاد فضا برای افرادی با تفکر و درک جدید نسبت به مساله» اشاره کرد. دیگری گفت: «هیات‌مدیره مسئولیت‌های سنگینی برای نظارت بر حوزه‌هایی که در مورد آنها تجربه زیادی ندارد، بر دوش می‌کشد که یکی از این حوزه‌ها امنیت سایبری است.»



شکل ۳-۴: امنیت سایبری بزرگ‌ترین چالش برای هیات‌مدیره است.

یک تهدید استراتژیک واقعی

هیات‌مدیره‌ها مسئولیت خود در خصوص موضوعات امنیت سایبری را نادیده می‌گیرند. در یک تحقیق انجام‌شده توسط «آی‌بی‌ام» تخمین زده شد که متوسط هزینه یک نشت داده حدود چهار میلیون دلار است. «سیسکو» در تحقیق اخیر خود اعلام کرد شرکت‌هایی که هدف حمله قرار گرفته‌اند، متحمل خسارت‌های شدیدی در درآمدها، مشتریان و فرصت‌های کسب‌وکاری

خود شده‌اند. واضح است که این حملات نمی‌توانند به‌عنوان یک تهدید خارجی انتزاعی در نظر گرفته شوند. هیات‌مدیره‌ها باید این حقیقت را بپذیرند و طرز فکر خود را تغییر دهند؛ تهدیدات امنیت سایبری جهانی است و اعضای هیات‌مدیره باید مسئولیت این ریسک‌ها را بر عهده بگیرند و این موضوع باید به‌طور منظم در تمام اتاق‌هـــای هیات‌مدیره، بدون توجه به صنعت، منطقه و اندازه شرکت، مورد بحث قرار گیرد.

هیات‌مدیره‌ها می‌توانند گام‌های محسوسی در حوزه امنیت سایبری و در نظر گرفتن آن به‌عنوان یکی از اولویت‌های شرکت بردارند. مدیران می‌توانند این کار را با «مطرح کردن سوالات و تعیین اینکه آیا فرایندهای مناســـب در جایگاه مناســـب قرار دارند یا خیر» آغاز کنند. هیات‌مدیره‌ها می‌توانند مدیریت اجرایی را مســـئول ارزیابی ریســـک‌های فعلی حوزه امنیت سایبری کنند و در نشســـت‌های هیات‌مدیره به‌طور منظم در این خصوص به بحث و تبادل نظر بپردازند. آنها می‌توانند از سرمایه‌گذاری در خصوص امنیت داده‌ها و زیرساخت‌های امنیتی درون‌سازمانی حمایت و همچنین در صورت لزوم مدیریت اجرایی را به دعوت از کارشناسان خارج از سازمان ترغیب کنند. این نوع ســـرمایه‌گذاری باید برای کارکردها و استراتژی‌های بلندمدت مدیریت ریسک سازمان حیاتی تلقی شود و آنها باید به‌طور مداوم مورد بررسی قرار گیرند. دامنه تهدیدات سایبری روزبه‌روز گسترده‌تر خواهد شد. بنابراین مدیران می‌توانند با اتخاذ رویکردی فعالانه در خصوص مسائل امنیت ســـایبری، نقش مهمی در حفاظت از ثبات سازمان خود و حمایت از رشد آتی آن ایفا کنند.

جمع‌بندی

هیات‌مدیره‌ها به اندازه کافی روی مسائل امنیت سایبری متمرکز نیستند که دلایل این موضوع و راهکارهایی برای آن در اینجا آورده شده است:

- بسیاری از هیات‌مدیره‌ها فاقد فرایندهای قوی برای گفت‌وگوی منظم در مورد ریسک‌های سایبری و بررسی برنامه‌های احتمالی برای یک نشت داده هستند.
- مدیران احساس می‌کنند تخصص لازم برای رســـیدگی به ریسک‌ها و مسائل امنیتی را ندارند.
- هیات‌مدیره‌ها باید این حقیقت را بپذیرند که تهدیدات امنیت سایبری جهانی هستند و

آنها باید مسئولیت این ریسک‌ها را بر عهده بگیرند.

- هیات‌مدیره‌ها می‌توانند با به‌کارگیری شیوه‌های متعدد، امنیت سایبری را در اولویت خود قرار داده و به مسائل آن رسیدگی کنند، از جمله:
  - افزایش پرسش‌های مرتبط با امنیت سایبری، حتی اگر پاسخ آنها را نمی‌دانند؛
  - قرار دادن موضوع امنیت سایبری در دستور کار منظم جلسات هیات‌مدیره؛
  - حمایت از سرمایه‌گذاری در امنیت داده‌ها و زیرساخت‌های مدیریت ریسک درون سازمان؛
  - دعوت از کارشناسان خارجی حوزه امنیت سایبری به‌عنوان مشاور یا یکی از اعضای هیات‌مدیره.

٤. چرا مدیران اجرایی روی امنیت سایبری سرمایه‌گذاری نمی‌کنند؟

الکس بلو

تعیین نرخ بازگشت سرمایه (ROI) برای هر سرمایه‌گذاری در امنیت سایبری؛ از آموزش کارکنان گرفته تا مدیران احراز هویت مجهز به هوش مصنوعی، به بهترین وجه می‌تواند به‌عنوان یک معمای حل‌نشده توصیف شود. چشم‌انداز تهدید دیجیتال به‌طور مداوم تغییر می‌کند و آگاهی از احتمال موفقیت یک حمله خاص و تعیین میزان خسارت‌های احتمالی بسیار دشوار است. حتی هزینه‌های شناخته‌شده مانند جریمه‌های نشت اطلاعات در صنایع به‌شدت قانون‌گذاری‌شده‌ای مانند بهداشت و درمان، بخش کوچکی از محاسبه ROI است. در صورت فقدان داده‌های مناسب، تصمیم‌گیرندگان باید از معیاری نه‌چندان کامل برای سنجش قابلیت‌ها استفاده کنند؛ قضاوت خود.

اما بینش‌های برگرفته از اقتصاد و روان‌شناسی رفتاری نشان می‌دهد که معمولا قضاوت انسانی مغرضانه است. در مورد امنیت سایبری، بعضی از تصمیم‌گیرندگان از مدل‌های ذهنی اشتباه جهت تعیین میزان و محل سرمایه‌گذاری استفاده می‌کنند. برای مثال، آنها ممکن است دفاع سایبری را به‌عنوان یک فرایند مستحکم‌سازی تلقی کنند (اگر شما یک دیواره دفاعی قدرتمند با برج‌های دارای نیروی کافی ایجاد کنید، می‌توانید مهاجمان را از یک مایل دورتر مشاهده کنید) یا ممکن است فرض کنند رعایت یک چارچوب امنیتی مانند NIST (موسسه مالی استانداردها و فناوری) یا FISMA (قانون نوسازی امنیتی اطلاعات فدرال)[1] به معنای سطح کافی امنیت است (اگر صرفا همه الزامات را رعایت کنید، می‌توانید مهاجمان آزاررسان را دور نگه دارید). همچنین آنها ممکن است نتوانند تفکر خلاف واقعی را مدنظر قرار دهند (ما امسال حتی یک نشت هم نداشتیم، پس نیازی به افزایش میزان سرمایه‌گذاری نداریم)، در حالی که در واقعیت آنها احتمالا امسال با خوش‌شانسی روبه‌رو بودند یا نسبت به یک عامل مخرب که در سیستم‌شان

1. Federal Information Security Modernization Act

کمین کرده و درصدد حمله است، غافل هستند.

مشکل این مدل‌های ذهنی آن است که با امنیت سایبری به‌عنوان یک مساله تمام‌شدنی قابل حل به جای یک فرایند مستمر و همیشگی رفتار می‌کنند. مهم نیست که یک شرکت چقدر ممکن است مستحکم باشد، هکرها بالاخره راهی پیدا خواهند کرد. به همین دلیل است که اقدامات امنیت سایبری باید بر مدیریت ریسک و نه کاهش ریسک متمرکز باشد، اما پذیرش این چشم‌انداز بدبینانه دشوار است. مدیران امنیتی چگونه می‌توانند از این طرز فکر گمراه‌کننده که به عدم سرمایه‌گذاری منجر می‌شود، اجتناب کرده و منابع مورد نیاز خود را ایمن کنند؟

شرکت تحقیق و طراحی علوم رفتاری من (ideas42) با متخصصان فضای امنیت سایبری مصاحبه‌هایی را صورت داده و در حال انجام تحقیقات گسترده‌ای برای شناسایی چالش‌های رفتاری انسان‌ها در سطح مهندسان، کاربران نهایی، مدیران فناوری اطلاعات و مدیران اجرایی است. ما به مسائلی از جمله اینکه چرا افراد در کدنویسی دچار اشتباه می‌شوند یا نمی‌توانند به‌روزرسانی‌های نرم‌افزار را نصب کنند و به‌صورت ضعیف مجوزهای دسترسی را مدیریت می‌کنند، وارد نشده‌ایم (ما این قبیل موضوعات را به‌صورت عمیق در گزارشی تحت عنوان «داستان امنیت سایبری، یک رمان مبتنی بر تحقیق» بررسی کرده‌ایم). یافته‌های ما به اقداماتی می‌پردازد که مدیران امنیتی و دیگر کارشناسان حوزه امنیت سایبری، می‌توانند جهت ارائه راه‌های جایگزین در برابر سوگیری‌های انسانی مدیران عامل و تشویق تصمیم‌گیران به سرمایه‌گذاری بیشتر در زیرساخت‌های سایبری انجام دهند.

به احساسات تصمیم‌گیران امور مالی متوسل شوید

نحوه انتقال اطلاعات، تاثیر زیادی بر چگونگی دریافت و عمل به آنها دارد. برای کارشناسان حوزه امنیت سایبری، توصیف ریسک سایبری از نظر یکپارچگی، دسترس‌پذیری داده‌ها یا معیارهای قابل اندازه‌گیری مانند میزان اتلاف بسته[1]، قابل درک است، اما این مفاهیم احتمالا تایید تصمیم‌گیرانی که در مورد ریسک به گونه دیگری فکر می‌کنند را به همراه ندارد. در عوض، کارشناسان حوزه امنیت سایبری باید اطلاعاتی که پیامدها را به‌روشنی به تصویر می‌کشد و به اصطلاح «به مذاق آنها بیشتر خوش می‌آید» را ارائه دهند. برای کنترل این «اثر سوگیری»،

1. Packet loss

کارشناسان امنیتی باید ریسک سایبری را از طریق گزارش‌های صریح مرتبط با حوزه‌های ریسکی که تصمیم‌گیران سطح بالا با آنها آشنا بوده و در حال حاضر عمیقا به آن توجه دارند، توضیح دهند. به‌عنوان مثال، حوزه ریسک شرکت شما ممکن است شـــامل از دست دادن داده‌های مشتری، هزینه‌های رگولاتوری و پیامدهای منفی مرتبط با روابط عمومی باشد که می‌تواند اعتبار شرکت را تحت تاثیر قرار دهد. این موضوع فقط در مورد آسیب‌دیدن داده‌ها نیست؛ بلکه به این مساله نیز اشاره دارد که داده‌های نامطلوب چگونه کارایی عملیاتی را کاهش خواهند داد و در خطوط تولید وقفه ایجاد خواهند کرد.

مدل ذهنی مدیرعامل خود را با معیارهـــای موفق جدید جایگزین کنید

افراد از مدل‌های ذهنی برای کاهش پیچیدگی مسائل و قابل کنترل کردن آنها استفاده می‌کنند. داشتن یک مدل ذهنی نادرســـت در مورد اینکه یک برنامه امنیت سایبری چه کاری قرار است انجام دهد، می‌تواند تفاوت بین یک حمله خنثی‌شده و یک نشت قابل توجه را رقم بزند. بعضی از مدیران اجرایی ارشد ممکن است فکر کنند سرمایه‌گذاری امنیتی به‌منظور ایجاد یک زیرساخت است و ایجاد یک قلعه مستحکم تمام آن چیزی است که برای ایمن نگه‌داشتن شرکت لازم است. با این تصویر ذهنی، اهداف یک تصمیم‌گیرنده امور مالی همواره به جای مدیریت ریســـک به سمت کاهش ریسک گرایش پیدا خواهد کرد.

برای رها شدن از این مساله، مدیران ارشـــد امنیت اطلاعات (CISOs) باید با هیات‌مدیره و تصمیم‌گیران جهت بازطراحی شـــاخصه‌های موفقیت از نظر تعداد نقاط آسیب‌پذیر کشف و برطرف‌شده همکاری کنند. هیچ سیستم امنیت ســـایبری‌ای غیر قابل نفوذ نخواهد بود، پس تلاش برای یافتن شکاف‌ها، تمرکز رهبران را از ایجاد سیستم درست به ایجاد فرایند درست تغییر خواهد داد. بر خلاف انتظار، عدم پوشش بیشتر نقاط آسیب‌پذیر توسط تیم امنیتی یک شرکت باید به‌عنوان نشانه‌ای مثبت تلقی شود. همه سیستم‌ها دارای اشکالاتی هستند و همه انسان‌ها می‌توانند هک شـــوند، پس در نظر گرفتن نقاط آســـیب‌پذیر به‌عنوان نقص باعث ایجاد انگیزه ناخواسته در تیم امنیتی داخلی جهت مخفی‌سازی آن خواهد شد. به این نکته توجه داشته باشید که هرچه فرایندهای امنیتی و قابلیت‌های تیم قوی‌تر باشد، نقاط آسیب‌پذیر بیشتری را کشف (و

برطرف) خواهند کرد.

بررسی همتایان خود به‌منظور تسهیل مهار اعتمادبه‌نفس کاذب

اعتمادبه‌نفس کاذب یک نوع سوگیری فراگیر است و اگر قضاوت رهبران در مورد سرمایه‌گذاری در حوزه امنیت سایبری را تحت تاثیر قرار دهد، می‌تواند به مشکل بزرگی تبدیل شود. تحقیقات ما نشان داده که بسیاری از مدیران اجرایی عالی‌رتبه معتقدند که سرمایه‌گذاری‌هایشان در حوزه امنیت سایبری کافی است، اما در حقیقت تعداد کمی از همتایان آنها در حال سرمایه‌گذاری به میزان مطلوبی هستند. یکی از راه‌هایی که مدیران ارشد امنیت اطلاعات می‌توانند از طریق آن بر اعتمادبه‌نفس کاذب مدیران ارشد اجرایی غلبه کنند، این است که عملکرد شرکت را با شرکت‌های مشابه مقایسه کنند. به عبارت دیگر، با مشکل به‌صورت مستقیم رودررو شوند. شما می‌توانید این کار را با نظرخواهی منظم از مدیران ارشد امنیت اطلاعات و مدیران اجرایی، در رابطه با اینکه سازمان‌ها در صنعت‌تان چگونه زیرساخت‌های امنیت سایبری را مدیریت می‌کنند، تشویق آنها به داشتن صراحت در مورد آنچه آنها به‌خوبی انجام می‌دهند یا انجام نمی‌دهند و درخواست از همان مدیران ارشد امنیت اطلاعات برای کمک به تعیین چگونگی عملکرد شرکت خود، انجام دهید. به این ترتیب، مدیران ارشد امنیت اطلاعات می‌توانند اطلاعات شفاف‌تری را به مدیران عامل در مورد چگونگی عملکرد آنها در مقایسه با همتایان صنعتی‌شان ارائه دهند.

شما ضعیف‌ترین لینک هستید

سوزان سانتاگ در کتاب خود با عنوان «تماشای درد دیگران» بیان کرده که «عکاسی یعنی قاب‌بندی و این قاب یعنی چشم‌بستن بر چیزهای دیگر». توجه انسان نیز تقریبا به همین شکل عمل می‌کند. افراد بر جنبه‌های خاصی از اطلاعات در محیط خود متمرکز می‌شوند و در عین حال موارد دیگر را نادیده می‌گیرند. آن حوزه‌ای که یک مدیر اجرایی ارشد برای سرمایه‌گذاری انتخاب می‌کند نیز می‌تواند بر همین مبنا باشد. به‌طور مثال، در پی وقوع یک هک قابل توجه، مدیران عامل ممکن است تیم‌های خود را به افزایش سرمایه‌گذاری در زیرساخت‌های سایبری به‌منظور حفاظت در برابر تهدیدات خارجی وادار کنند، اما با این کار ممکن است از تهدیدات

داخلی ناخواسته‌ای غافل شـــوند که احتمالا به همان اندازه هزینه‌بر است؛ کارکنانی که روی لینک‌های بد در مرورگرهای اینترنتی کلیک می‌کنند یا قربانی حملات فیشینگ می‌شوند.

یک مدیر ارشـــد امنیت اطلاعات چگونه می‌تواند راهکاری برای حل مشـــکل بی‌توجهی تصمیم‌گیران پیدا کند؟ هیچ‌کس دوست ندارد شرمنده شود، اما بازخورد منفی گاهی می‌تواند راهکار موثری برای بی‌توجهی باشـــد. تیم‌های امنیتی باید به‌طور منظم تلاش کنند تا از طریق آزمایش به سیستم‌های خود نفوذ کنند و باید سامانه‌های مرتبط با مدیران عامل مهم‌ترین هدف آنها باشـــد و این کار را دقیقا به همان صورت که هکرها از بیرون به سیستم نگاه می‌کنند، انجام دهند؛ زیرا با قربانی کردن مدیر ارشد اجرایی در یک حمله عامدانه (و ایمن) داخلی، ممکن است توجه آنها به ریسک‌های بالقوه‌ای که در حال حاضر وجود دارد، جلب شود و بنابراین رهبران را به افزایش سرمایه‌گذاری در زیرساخت‌های سایبری ترغیب کند.

اگر برنامه‌های امنیت سایبری کماکان بر طراحی فناوری‌های بهتر جهت مقابله با تهدیدات روزافزون حملات سایبری تمرکز داشته باشـــند، ما نیز به غفلت خود نسبت به مهم‌ترین جنبه امنیت، یعنی اشخاص میانی، ادامه خواهیم داد. با تغییر نگرش علوم رفتاری به سمت چالش‌های امنیت سایبری، مدیران ارشد امنیت اطلاعات می‌توانند شـــیوه‌های جدیدی را برای مقابله با مشکلات قدیمی شناسایی کرده و شاید در همین حین بودجه‌های اختصاص‌داده خود به این حوزه را اصلاح کنند.

جمع‌بندی

تصمیم‌گیران که امنیت سایبری را به چشم یک مشکل تمام‌شدنی و قابل حل می‌بینند تا یک فرایند در جریان که نیازمند به‌روزرسانی و نوسازی مداوم است؛ نیازمند مدل‌های ذهنی جدیدی برای تعیین میزان و محل سرمایه‌گذاری در حوزه امنیت سایبری هستند:

- کارشناسان حوزه امنیت ســـایبری باید اثر ســـوگیری را از طریق گزارش‌های مرتبط با حوزه‌های ریسک، مانند از دست دادن داده‌های مشتری و هزینه‌های رگولاتوری که هم‌اکنون تصمیم‌گیران سطح بالا به آنها توجه دارند (گرایش افراد در داشتن توجه بیشتر به اطلاعاتی که پیامدها را به‌طور واضح نشان می‌دهد و بیشتر به مذاق آنها خوش می‌آید) کنترل کنند.
- بازطراحی معیارهای موفقیت: تمرکز بر ایجاد فرایند درست به جای سیستم درست. تعداد

نقاط آسیب‌پذیری که تیم امنیتی آنها را پوشش نمی‌دهد، به‌عنوان یک برگ برنده قلمداد شود؛ نه یک شکست.

- مهار اعتماد به نفس کاذب با ارائه اطلاعاتی توسط مدیران ارشد امنیت اطلاعات در مورد چگونگی عملکرد شرکت از لحاظ امنیت سایبری در مقایسه با همتایان صنعتی.
- از طریق یک حمله عامدانه (و ایمن) داخلی، مدیران ارشد اجرایی خود را هدف قرار دهید تا توجه آنها را به ریسک‌های بالقوه موجود جلب کرده و رهبران را به افزایش سرمایه‌گذاری در زیرساخت‌ها ترغیب کنید.

۵. چرا مدیران ارشد باید از معیارهای یکسانی برای ارزیابی ریسک سایبری استفاده کنند؟

جیسون جی هاگ

وقتی موضوع امنیت سایبری در میان باشد، زنجیره ارتباطات درون یک سازمان (اگر اصلا چنین چیزی وجود داشته باشد)، اغلب موجب آشفتگی می‌شود. در بسیاری از بخش‌های سازمان مباحث متعددی به‌صورت جداگانه در رابطه با ریسک‌های سایبری صورت می‌گیرد. در همین حین، مدیران ارشد که با استفاده از معیارهای مختلفی (مالی، رگولاتوری، فنی، عملیاتی) در حال سنجش نقاط آسیب‌پذیر بالقوه سازمان هستند، موجب ایجاد ارزیابی‌های متناقضی می‌شوند. مدیران عامل باید با ایجاد فرهنگی که ارتباطات باز را تقویت می‌کند، شفافیت در مورد نقاط آسیب‌پذیر را افزایش می‌دهد و همچنین مشارکت در تعیین نقاطی که نشت اطلاعاتی در آنجا صورت گرفته؛ این ناپیوستگی‌ها را شناسایی کنند.

سازمان‌ها با هر اندازه‌ای در تمام بخش‌ها در حال تجربه یک افزایش تصاعدی در میزان مواجهه با ریسک سایبری هستند. از آنجایی که مشتریان خواستار تعاملات دیجیتال و دستگاه‌های هوشمند بیشتری هستند، تعداد نقاط انتهایی نیازمند حفاظت، شدیدا رو به افزایش است. («سیسکو» و «سایبرسکیوریتی ونچرز» در سالنمای سال ۲۰۱۹ خود در مورد امنیت سایبری پیش‌بینی کردند که تعداد دستگاه‌های متصل به اینترنت تا سال ۲۰۲۰ از ۵۰ میلیارد فراتر خواهد رفت.) دشمنان از بازیگران بدی که به‌صورت مستقل فعالیت می‌کردند، به گروه‌ها و دولت‌های بسیار توانمند و سازمان‌یافته تبدیل شده‌اند. چشم‌انداز رگولاتوری به‌طور فزاینده‌ای در حال تغییر است و در بعضی موارد با سطوح محلی، ملی و بین‌المللی در تناقض قرار می‌گیرد. حملات سایبری معروف (از حمله به شرکت سونی پیکچرز در سال ۲۰۱۴ تا حملات باج‌افزاری که در سال ۲۰۱۶ رخ داد) خسارات زیادی را به لحاظ مالی و اعتباری به بار آورده‌اند.

مدیران عاملی که قصد دارند این تهدیدات رو به‌رشد را تحت کنترل درآورند، باید ابعاد کلی

ریسک‌های درون شرکت را ارزیابی کرده و به‌طور همه‌جانبه این نقاط در معرض ریسک را شناسایی کنند؛ چراکه عواقب عدم انجام چنین اقداماتی می‌تواند به سلب اعتماد ذی‌نفعان، مشتریان و حتی از دست رفتن مشاغل‌شان منجر شود.

مدیران ارشد یک سازمان اغلب زبان مشترکی در رابطه با ریسک سایبری ندارند. برای مثال، مشاور حقوقی این مساله را از منظر انطباق با مقررات امنیت اطلاعات مانند مقررات عمومی حفاظت از داده اتحادیه اروپا (GDPR) بررسی می‌کند. مدیر ارشد امنیت اطلاعات (CISO) یا مدیر ارشد فناوری اطلاعات (CIO) فقط نقاط آسیب‌پذیری را گزارش می‌کنند که موفق به اصلاح آنها شده‌اند. مدیر ارشد ریسک (CRO) از نظر انتقال ریسک و بیمه سایبری خریداری‌شده به این مشکل نگاه می‌کند و مدیر مالی ارشد تاثیر مالی بالقوه آن را بررسی می‌کند.

این فقدان ارتباطات و هماهنگی در کارکردها، ارزیابی کلی میزان تاثیر ریسک سایبری بر کسب‌وکار یا ایجاد معیارهای مشترک برای انجام این کار را بسیار دشوار می‌سازد. این موضوع اولویت‌بندی ریسک‌هایی که باید هرچه سریع‌تر به آنها رسیدگی شود را با مشکل مواجه می‌کند و در عین حال هدایت مناسب اقدامات و منابع را چالش‌برانگیزتر می‌سازد.

بنابراین مدیران عامل باید برای ایجاد یک زبان مشترک در مورد امنیت سایبری در سازمان‌های خود گام‌های متعددی بردارند.

گام اول این است که مدیران عامل باید مدیران ارشد یک سازمان را گرد هم جمع کنند تا همه ذی‌نفعان سازمان به‌منظور ایجاد یک تصویر واقع‌بینانه و یکپارچه از نقاط در معرض ریسک کسب‌وکار، با هم ارتباط برقرار کرده و همکاری کنند. این گام شامل این موارد است: شناسایی داده‌ها و دارایی‌های حیاتی که می‌توانند در معرض ریسک باشند؛ ارزیابی نقاط آسیب‌پذیر فنی؛ درک دورنمای تهدید؛ ارزیابی پیامدهای رگولاتوری و انطباق با قوانین بالقوه حملات سایبری؛ سنجش پیامدهای مالی حملات (از جمله هزینه‌های وقفه در کسب‌وکار، هزینه‌های اصلاح، کاهش ارزش سرمایه‌گذاری، آسیب به برند و اعتبار) و دستیابی به تصویری دقیق‌تر از تاثیر حملات بر ارزش سهام شرکت.

گام دوم، ایجاد فرهنگی است که کارکنان را به بیان صریح نظرات خود در مورد مواجهه با ریسک سایبری، بدون ترس از واکنش‌های منفی، ترغیب می‌کند. این اقدام نادری است که یک مدیرعامل، مدیران ارشد شرکت را (به‌خصوص مدیر ارشد امنیت اطلاعات یا مدیر ارشد

ریسک) تشویق کند که گزارش‌های مستمری از رشد نقاط در معرض ریسک شرکت تهیه کنند. از آنجا که ریسک سایبری پویاست، مدیران عامل باید محیطی ایجاد کنند که در آن گفت‌وگوهای پیوسته‌ای در رابطه با پیامدهای امنیتی روندهای جدید (معرفی فناوری‌ها و سیستم‌های جدید، تهدیدات سایبری جدید، ادغام‌ها و تملیک‌ها که شامل ترکیب سیستم‌های اطلاعاتی و فرهنگ امنیت سازمان‌های مختلف می‌شود) صورت گیرد.

به‌عنوان بخشی از این اقدامات، مدیران عامل باید به‌صورت فعال با کارکنانی که در بخش امنیتی سازمان فعالیت می‌کنند، گفت‌وگو کنند. هرچه مدیران عامل بیشتر با مهندسان سیستم و تیم‌های فنی ارتباط برقرار کنند، راحت‌تر می‌توانند از آنها در مورد امنیت سازمان سوال کنند. اگر مدیر ارشد ریسک و مدیر ارشد امنیت اطلاعات تنها در مورد اتفاقات خوب گزارش ارائه دهند، پس باید زنگ خطر به صدا در بیاید.

سومین گام این است که مدیران عامل باید به‌منظور آمادگی در برابر حملات سایبری اطمینان حاصل کنند که هر کس وظیفه خود را می‌داند و می‌تواند در طول یک حادثه به‌صورت کارآمد با سایر افراد ارتباط برقرار کند. باید یک برنامه واکنش به حوادث سایبری وجود داشته باشد که به‌طور منظم از طریق حملات شبیه‌سازی‌شده مورد آزمایش قرار گیرد تا بتواند نقاط آسیب‌پذیر شرکت را نیز مورد آزمایش قرار دهد. داشتن یک برنامه می‌تواند در صورت وقوع حمله، اختلال در کسب‌وکار را به حداقل برساند و طول دوره‌ای که مهاجمان به سرقت داده‌های حیاتی یا پول می‌پردازند و همچنین میزان خسارت را کاهش دهد. یک برنامه واکنش به حوادث باید شامل این مراحل باشد: آماده‌سازی؛ شناسایی و تجزیه‌وتحلیل؛ مهار و بازیابی؛ پساحادثه.

مرحله آماده‌سازی مهم‌ترین مرحله است؛ زیرا ایجاد یک برنامه واکنشی در طول یک حادثه کارساز نخواهد بود. برنامه‌ریزی به تمام ذی‌نفعان در درک نقش و مسئولیت‌های خود کمک می‌کند؛ از این موضوع که چه چیزی یک حادثه امنیتی را ایجاد می‌کند گرفته تا اینکه چه کسی برنامه را آغاز می‌کند. همچنین این کار در طول یک حادثه به مدیریت برقراری ارتباط مطمئن در داخل؛ با مدیران ارشد و اعضای هیات‌مدیره و در خارج؛ با مشتریان، مشاوران خارجی، شرکت‌های بیمه، رگولاتورها و مراجع قانونی کمک می‌کند.

در مرحله شناسایی و تجزیه‌وتحلیل، تیم امنیتی دامنه حادثه را تعیین و داده‌های مورد نیاز برای انجام تجزیه‌وتحلیل‌ها را جمع‌آوری می‌کند. مرحله سوم مهار حادثه است؛ جلوگیری از گسترش

حمله با از بین بردن هر گونه آلودگی از سیستم و رفع تمام نقاط آسیب‌پذیر کشف‌شده. مرحله پساحادثه شامل بررسی این موارد است: چه اقداماتی خوب پیش رفت، چه اقداماتی با مشکل روبه‌رو شد و دفعه بعد چه اقداماتی را می‌توان بهتر انجام داد.

کارشناسان حوزه امنیت سایبری که خارج از سازمان هستند، می‌توانند به توسعه این برنامه کمک کنند، اما مدیرعامل باید آزمایش‌های متعددی برای تست میزان کارایی و تاثیرگذاری این برنامه انجام دهد تا مطمئن شود در زمان بروز حادثه این برنامه به‌خوبی عمل می‌کند.

در نهایت شرکت‌ها باید یک واحد داخلی تعریف کنند که مسئول آن به‌طور منظم میزان آمادگی شرکت در برابر حوادث امنیتی را بررسی کند. این واحد که به‌طور مستقیم به مدیرعامل گزارش می‌دهد، باید حملات شبیه‌سازی‌شده به کسب‌وکار را نیز سامان‌دهی کند. همچنین واحد مذکور باید از کارشناسان سایبری خارج از سازمان که دیدگاه‌های به‌روزی در مورد جدیدترین شیوه‌های امنیت سایبری، تهدیدات و روندها دارند، بهره ببرد تا بتواند چشم‌اندازهای عاری از تعصبی ارائه و در صورت لزوم تصمیمات مدیریتی را به چالش بکشد.

یک مدیرعامل باید از تمام ظرفیت‌ها برای ایجاد معیارهای مشترک برای ارزیابی ریسک‌های سایبری استفاده کند تا همه افراد دیدگاه یکسانی در مورد آن داشته باشند و همچنین باید یک فرهنگ امنیت سایبری را از طریق گفت‌وگوی آزاد، برنامه‌ریزی و آزمایش ایجاد کند. در صورت انجام این کارها وقتی او در مورد ریسک‌های سایبری سوالاتی را مطرح می‌کند (مانند «بزرگ‌ترین ریسک شرکت ما چیست؟»، «دارایی‌های حیاتی ما کدام است؟»، «چه کسی به آنها دسترسی دارد؟»، «سیاست امنیت اطلاعات فعلی ما چیست؟»، «برنامه واکنش به حوادث ما چیست؟»، «این برنامه آخرین بار چه زمانی مورد آزمایش قرار گرفت؟ و...)، پاسخ‌های کارکنان تصویر دقیق‌تری را ترسیم خواهد کرد.

یک مدیرعامل تنها وقتی می‌تواند تخصیص منابع برای مدیریت این ریسک‌ها را اولویت‌بندی کند که خطر واقعی ریسک‌های سایبری را کاملا درک کند.

جمع‌بندی

مدیران عامل باید برای ارزیابی، اولویت‌بندی و مواجهه با ریسک‌های سایبری به یک زبان مشترک در سازمان برسند و اقدامات زیر را انجام دهند:

- تمام مدیران و شـــرکا را گرد هم آورید تا تصویر واقع‌بینانه و یکپارچـــه‌ای از مواجهه با ریسک‌ها ترسیم کنید.
- فرهنگی را ایجاد کنید که در آن کارکنان بتوانند به‌راحتی گفت‌وگوهای مستمری در مورد موضوعاتی مانند مواجهه با ریسک سایبری، فناوری‌ها و سیســـتم‌های جدید و تاثیر یک ادغام و تملک بر سیستم‌های اطلاعاتی و فرهنگ امنیتی سازمان‌های هدف، انجام دهند.
- با تهیه یک برنامه واکنشی و طراحی حملات شبیه‌سازی‌شده به‌صورت منظم، آمادگی همه کارکنان را برای مواجهه با حملات سایبری محک بزنید.
- پیگیری‌های منظمی در مورد میزان آمادگی شـــرکت در برابر ریسک‌های امنیتی انجام دهید.

چیزی ندیده‌ام هنوز

► HBR's latest thinking on
the future of business

Insights You Need from

Harvard Business Review

CYBER SECURITY

بهسازان ملت
behsazan mellat

ISBN 978-622-97220-1-5
۴۱۵۰۰ تومان

انتشارات راه‌پرداخت